DoD 5400.11-R

Director of Administration and
Management, Office of the Secretary
of Defense

(703)614-3027

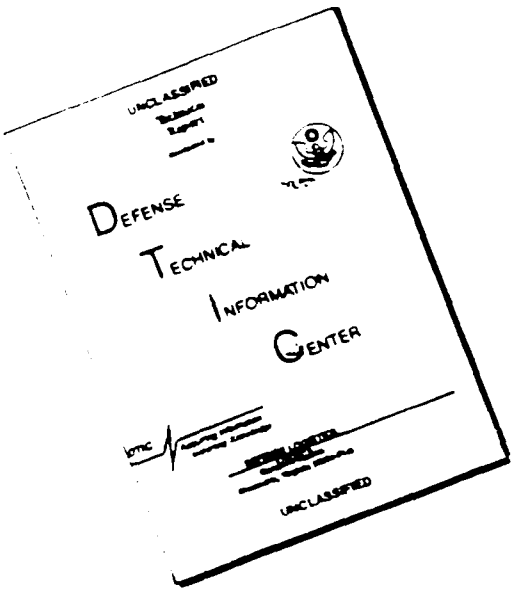
DEPARTMENT OF DEFENSE

PRIVACY PROGRAM

AUGUST 1983

DEPUTY ASSISTANT SECRETARY OF DEFENSE (ADMINISTRATION)

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

COMPTROLLER
(Administration)

DoD 5400.11-R

August 31, 1983

FOREWORD

This Regulation is issued under the authority of DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982. Its purpose is to prescribe uniform procedures for implementation of the Defense Privacy Program.

This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, and the Defense Agencies (hereafter referred to as "DoD Components"). It applies to the National Security Agency only to the extent that its provisions are not inconsistent with Public Laws 86-36 and 88-290.

The provisions of this Regulation shall be applicable by contract or other legally binding action to U.S. Government contractors whenever a DoD contract is let for the operation of a system of records or a portion of a system of records. For purposes of responsibilities under DoD Directive 5400.11, contractor employees shall be considered employees of the contracting DoD Component.

This Regulation does not apply to:

1. Requests for information made under the Freedom of Information Act (DoD Directive 5400.7). These are processed in accordance with DoD 5400.7-R, "DoD Freedom of Information Act Program," December 1980.

2. Requests for information from systems of records controlled by the Office of Personnel Management (OPM), although maintained by a DoD Component. These are processed under the applicable parts of the OPM's Federal Personnel Manual.

3. Requests for personal information from the General Accounting Office. These are processed in accordance with DoD Directive 7650.1, "General Accounting Office Access to Records," August 26, 1982.

4. Requests for personal information from Congress. These are processed in accordance with DoD Directive 5400.4, "Provision of Information to Congress," January 30, 1978, except for those specific provisions in Chapter 4 of this Regulation.

This Regulation is effective immediately and is mandatory for use by all DoD Components. Heads of DoD Components may issue supplementary instructions only when necessary to provide for unique requirements within their Components. Such instructions may not conflict with the provisions of this Regulation.

Forward recommended changes through appropriate channels to:

Director, Defense Privacy Office
OSD Mail Room, Room 3A-948
The Pentagon
Washington, D.C. 20301

DoD Components may obtain copies of this Regulation through their own publications channels. Other federal agencies and the public may obtain copies from the Director, U.S. Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.

D. O. Cooke
Deputy Assistant Secretary of Defense

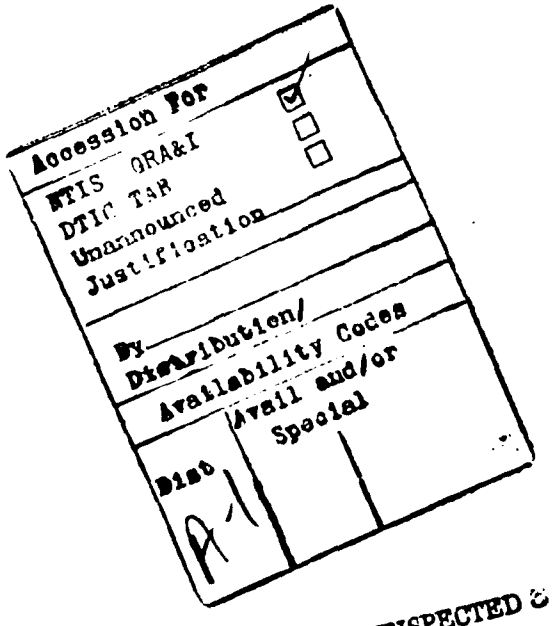


TABLE OF CONTENTS

REFERENCES

(a) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, June 7, 1982
(b) Title 5, United States Code, Section 552a, as amended, "The Privacy Act of 1974"
(c) Title 44, United States Code, Section 303a, "Examination by the Administrator of General Services of Lists and Schedules of Records Lacking Preservation Value, Disposal of Records"
(d) Defense Acquisition Regulation (DAR), Section 1.327, "Protection of Individual Privacy"
(e) Title 31, United States Code, Section 952(d), as amended, "The Federal Claims Collection Act of 1966"
(f) DoD 5400.7-R, "DoD Freedom of Information Act Program," December 1980, authorized by DoD Directive 5400.7, March 24, 1980
(g) Executive Order No. 9397, "Numbering System For Federal Accounts Relating to Individual Persons," November 30, 1943
(h) Office of Personnel Management, Federal Personnel Manual (5 CFR Parts 293, 294, 297, and 735)
(i) DoD Directive 5000.21, "Forms Management Program," December 5, 1973
(j) Title 5, United States Code, Section 552, "The Freedom of Information Act"
(k) Title 42, United States Code, Section 653
(l) Title 13, United States Code, Section 8
(m) DoD Directive 1344.9, "Indebtedness of Military Personnel," May 7, 1979
(n) Title 18, United States Code, Section 3056
(o) DoD 5025.1-M, "Directives System Procedures," April 1981, authorized by DoD Directive 5025.1, October 16, 1980
(p) DoD Directive 5400.9, "Publication of Proposed and Adopted Regulations Affecting the Public," December 23, 1974
(q) Transmittal Memorandum No. 1, Office of Management and Budget (OMB) Circular A-71, "Security of Federal Automated Information Systems," July 27, 1978
(r) DoD 5200.28-M, "ADP Security Manual," January 1973, authorized by DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972
(s) OMB Circular A-19, "Legislative Coordination and Clearance," as amended
(t) Title 5, United States Code, Section 55165, 5517, and 5520
(u) Treasury Fiscal Requirements Manual Bulletin No 76-07

DEFINITIONS

1. Access. The review of a record or a copy of a record or parts thereof in a system of records by any individual (see also paragraph 7., below).

2. Agency. For the purposes of disclosing records subject to the Privacy Act among DoD Components, the Department of Defense is a considered a single agency. For all other purposes to include applications for access and amendment, denial of access or amendment, appeals from denials, and record keeping as regards release to non-DoD agencies; each DoD Component is considered an agency within the meaning of the Privacy Act.

3. Confidential source. A person or organization who has furnished information to the federal government under an express promise that the person's or the organization's identity will be held in confidence or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

4. Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or government agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian.

5. Individual. A living citizen of the United States or an alien lawfully admitted to the United States for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf. No rights are vested in the representative of a dead person under this Regulation and the term "individual" does not embrace an individual acting in an interpersonal capacity (for example, sole proprietorship or partnership).

6. Individual access. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

7. Maintain. Includes maintain, collect, use, or disseminate.

8. Official use. Within the context of this Regulation, this term is used when officials and employees of a DoD Component have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties, subject to DoD 5200.1-R (reference (a)).

9. Personal information. Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life.

10. Privacy Act. The Privacy Act of 1974, as amended, 5 U.S.C. 552a (reference (b)).

11. Privacy Act request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records. The request must indicate that it is being made under the Privacy Act to be considered a Privacy Act request.

12. Member of the public. Any individual or party acting in a private capacity to include federal employees or military personnel.

13. Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

14. Risk assessment. An analysis considering information sensitivity, vulnerabilities, and the cost to a computer facility or word processing activity in safeguarding personal information processed or stored in the facility or activity.

15. Routine use. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.

16. Statistical record. A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

17. System of records. A group of records under the control of a DoD Component from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all Privacy Act systems of records must be published in the Federal Register.

18. Word processing system. A combination of equipment employing automated technology, systematic procedures, and trained personnel for the primary purpose of manipulating human thoughts and verbal or written communications into a form suitable to the originator. The results are written or graphic presentations intended to communicate verbally or visually with another individual.

19. Word processing equipment. Any combination of electronic hardware and computer software integrated in a variety of forms (firmware, programable software, hardwiring, or similar equipment) that permits the processing of textual data. Generally, the equipment contains a device to receive information, a computer-like processor with various capabilities to manipulate the information, a storage medium, and an output device.

CHAPTER 1

SYSTEMS OF RECORDS

A. GENERAL

1. System of records. To be subject to the provisions of this Regulation a "system of records" must

a. Consist of "records" (as defined in paragraph 13, page xii) that are retrieved by the name of an individual or some other personal identifier, and

b. Be under the control of a DoD Component.

2. Retrieval practices

a. Records in a group of records that may be retrieved by a name or personal identifier are not covered by this Regulation even if the records contain personal data and are under control of a DoD Component. The records must be, in fact, retrieved by name or other personal identifier to become a system of records for the purpose of this Regulation.

b. If files that are not retrieved by name or personal identifier are rearranged in such manner that they are retrieved by name or personal identifier, a new systems notice must be submitted in accordance with subsection D.3. of Chapter 6.

c. If records in a system of records are rearranged so that retrieval is no longer by name or other personal identifier, the records are no longer subject to this Regulation and the system notice for the records shall be deleted in accordance with subsection E.3. of Chapter 6.

3. Relevance and necessity. Retain in a system of records only that personal information which is relevant and necessary to accomplish a purpose required by a federal statute or an Executive Order.

4. Authority to establish systems of records. Identify the specific statute or the Executive Order that authorizes maintaining personal information in each system of records. The existance of a statute or Executive order mandating the maintenance of a system of records does not abrogate the responsibility to ensure that the information in the system of records is relevant and necessary.

5. Exercise of First Amendment rights

a. Do not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution except when:

(1) Expressly authorized by federal statute;

(2) Expressly authorized by the individual; or

(3) Maintenance of the information is pertinent to and within the scope of an authorized law enforcement activity.

b. First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

6. System manager's evaluation

a. Evaluate the information to be included in each new system before establishing the system and evaluate periodically the information contained in each existing system of records for relevancy and necessity. Such a review shall also occur when a system notice amendment or alteration is prepared (see sections D. and E. of Chapter 6).

b. Consider the following:

(1) The relationship of each item of information retained and collected to the purpose for which the system is maintained;

(2) The specific impact on the purpose or mission of not collecting each category of information contained in the system;

(3) The possibility of meeting the informational requirements through use of information not individually identifiable or through other techniques, such as sampling;

(4) The length of time each item of personal information must be retained;

(5) The cost of maintaining the information; and

(6) The necessity and relevancy of the information to the purpose for which it was collected.

7. Discontinued information requirements

a. Stop collecting immediately any category or item of personal information for which retention is no longer justified. Also excise this information from existing records, when feasible.

b. Do not destroy any records that must be retained in accordance with disposal authorizations established under 44 U.S.C., Section 303a (reference (c)).

B. STANDARDS OF ACCURACY

1. Accuracy of information maintained. Maintain all personal information that is used or may be used to make any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in making any such determination.

2. Accuracy determinations before dissemination. Before disseminating any personal information from a system of records to any person outside the Depart-

ment of Defense, other than a federal agency, make reasonable efforts to ensure that the information to be disclosed is accurate, relevant, timely, and complete for the purpose it is being maintained (see also subsection A.4. of Chapter 3 and subsection A.4. of Chapter 4).

C. GOVERNMENT CONTRACTORS

1. Applicability to government contractors

a. When a DoD Component contracts for the operation or maintenance of a system of records or a portion of a system of records by a contractor, the record system or the portion of the record system affected are considered to be maintained by the DoD Component and are subject to this Regulation. The Component is responsible for applying the requirements of this Regulation to the contractor. The contractor and its employees are to be considered employees of the DoD Component for purposes of the sanction provisions of the Privacy Act during the performance of the contract. Consistent with the Defense Acquisition Regulation (DAR), section 1.327 (reference (d)), contracts requiring the maintenance of a system of records or the portion of a system of records shall identify specifically the record system and the work to be performed and shall include in the solicitation and resulting contract such terms as are prescribed by reference (d).

b. If the contractor must use or have access to individually identifiable information subject to this Regulation to perform any part of a contract, and the information would have been collected and maintained by the DoD Component but for the award of the contract, these contractor activities are subject to this Regulation.

c. The restriction in paragraphs C.1.a. and b. of this Chapter do not apply to records:

(1) Established and maintained to assist in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract;

(2) Maintained as internal contractor employee records even when used in conjunction with providing goods and services to the Department of Defense; or

(3) Maintained as training records by an educational organization contracted by a DoD Component to provide training when the records of the contract students are similar to and comingled with training records of other students (for example, admission forms, transcripts, academic counselling and similar records).

(4) Maintained by a consumer reporting agency to which records have been disclosed under contract in accordance with the Federal Claims Collection Act of 1966 (reference (e)).

d. DoD Components must publish instructions that:

(1) Furnish DoD Privacy Program guidance to their personnel who solicit, award, or administer government contracts;

(2) Inform prospective contractors of their responsibilities regarding the DoD Privacy Program; and

(3) Establish an internal system of contractor performance review to ensure compliance with the DoD Privacy Program.

2. Contracting procedures. The Defense Systems Acquisition Regulatory Council (DSARC) is responsible for developing the specific policies and procedures to be followed when soliciting bids, awarding contracts or administering contracts that are subject to this Regulation.

3. Contractor compliance. Through the various contract surveillance programs, ensure contractors comply with the procedures established in accordance with subsection C.2. of this Chapter.

4. Disclosure of records to contractors. Disclosure of personal records to a contractor for the use in the performance of any DoD contract by a DoD Component is considered a disclosure within the Department of Defense (see subsection A.2. of Chapter 4). The contractor is considered the agent of the contracting DoD Component and to be maintaining and receiving the records for that Component.

D. SAFEGUARDING PERSONAL INFORMATION

1. General responsibilities. Establish appropriate administrative, technical and physical safeguards to ensure that the records in every system of records are protected from unauthorized alteration or disclosure and that their confidentiality is protected. Protect the records against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

2. Minimum standards

a. Tailor system safeguards to conform to the type of records in the system, the sensitivity of the personal information stored, the storage medium used and, to a degree, the number of records maintained.

b. Treat all unclassified records that contain personal information that normally would be withheld from the public under Exemption Numbers 6 and 7, section 3-200, DoD 5400.7-R (reference (f)) as if they were designated "For Official Use Only" and safeguard them in accordance with the standards established by reference (f) even if they are not actually marked "For Official Use Only."

c. Afford personal information that does not meet the criteria discussed in paragraph D.3.b. of this Chapter that degree of security which provides protection commensurate with the nature and type of information involved.

d. Special administrative, physical, and technical procedures are required to protect data that is stored or being processed temporarily in an

automated data processing (ADP) system or in a word processing activity to protect it against threats unique to those environments (see Appendices A and B).

e. Tailor safeguards specifically to the vulnerabilities of the system.

3. Records disposal

a. Dispose of records containing personal data so as to prevent inadvertent compromise. Disposal methods such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

b. The transfer of large quantities of records containing personal data (for example, computer cards and printouts) in bulk to a disposal activity, such as the Defense Property Disposal Office, is not a release of personal information under this Regulation. The sheer volume of such transfers make it difficult or impossible to identify readily specific individual records (see paragraph D.3.c. of this Chapter).

c. When disposing of or destroying large quantities of records containing personal information, care must be exercised to ensure that the bulk of the records is maintained so as to prevent specific records from being readily identified. If bulk is maintained, no special procedures are required. If bulk cannot be maintained or if the form of the records make individually identifiable information easily available, dispose of the record in accordance with paragraph D.3.a. of this Chapter.

CHAPTER 2

COLLECTING PERSONAL INFORMATION

A. GENERAL CONSIDERATIONS

1. Collect directly from the individual. Collect to the greatest extent practicable personal information directly from the individual to whom it pertains if the information may be used in making any determination about the rights, privileges, or benefits of the individual under any federal program (see also subsection A.3. of this Chapter).

2. Collecting Social Security Numbers (SSNs)

a. It is unlawful for any federal, state, or local governmental agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, if a federal statute requires that the SSN be furnished or if the SSN is required to verify the identity of the individual in a system of records that was established and in use before January 1, 1975, and the SSN was required as an identifier by a statute or regulation adopted before that date, this restriction does not apply.

b. When an individual is requested to provide his or her SSN, he or she must be told:

(1) The uses that will be made of the SSN;

(2) The statute, regulation, or rule authorizing the solicitation of the SSN; and

(3) Whether providing the SSN is voluntary or mandatory.

c. Include in any systems notice for any system of records that contains SSNs a statement indicating the authority for maintaining the SSN and the sources of the SSNs in the system. If the SSN is obtained directly from the individual indicate whether this is voluntary or mandatory.

d. E.O. 9397 (reference (g)) authorizes solicitation and use of SSNs as numerical identifier for individuals in most federal records systems. However, reference (g) does not provide mandatory authority for soliciting SSNs.

e. Upon entrance into military service or civilian employment with the Department of Defense, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. Provide the notification in paragraph A.2.b. of this Chapter to the individual when originally soliciting his or her SSN. After an individual has provided his or her SSN for the purpose of establishing a record, the notification in paragraph A.2.b. is not required if the individual is only requested to furnish or verify the SSNs for identification purposes in connection with the normal use of his or her records. However, if the SSN is to be written down and retained for any purpose by the requesting official, the individual must be provided the notification required by paragraph A.2.b. of this Chapter.

f. Consult the FPM (reference (h)) when soliciting SSNs for use in OPM records systems.

3. Collecting personal information from third parties. It may not be practical to collect personal information directly from the individual in all cases. Some examples of this are:

a. Verification of information through third party sources for security or employment suitability determinations;

b. Seeking third party opinions such as supervisory comments as to job knowledge, duty performance, or other opinion-type evaluations;

c. When obtaining the needed information directly from the individual is exceptionally difficult or may result in unreasonable costs; or

d. Contacting a third party at the request of the individual to furnish certain information such as exact periods of employment, termination dates, copies of records, or similar information.

4. Privacy Act Statements

a. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement is required regardless of the medium used to collect the information (forms, personal interviews, stylized formats, telephonic interviews, or other methods). The Privacy Act Statement consists of the elements set forth in paragraph A.4.b. of this Chapter. The statement enables the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement need not be given. However, personal information obtained without a Privacy Act Statement shall not be incorporated into any system of records. When soliciting SSNs for any purpose, see paragraph A.2.b. of this Chapter.

b. The Privacy Act Statement shall include:

(1) The specific federal statute or Executive Order that authorizes collection of the requested information (see subsection A.4. of Chapter 1).

(2) The principal purpose or purposes for which the information is to be used;

(3) The routine uses that will be made of the information (see subsection B.6. of Chapter 4);

(4) Whether providing the information is voluntary or mandatory (see subsection A.5. of this Chapter); and

(5) The effects on the individual if he or she chooses not to provide the requested information.

c. The Privacy Act Statement shall be concise, current, and easily understood.

d. The Privacy Act statement may appear as a public notice (sign or poster), conspicuously displayed in the area where the information is collected, such as at check-cashing facilities or identification photograph facilities.

e. The individual normally is not required to sign the Privacy Act Statement.

f. Provide the individual a written copy of the Privacy Act Statement upon request. This must be done regardless of the method chosen to furnish the initial advisement.

5. Mandatory as opposed to voluntary disclosures. Include in the Privacy Act Statement specifically whether furnishing the requested personal data is mandatory or voluntary. A requirement to furnish personal data is mandatory only when a federal statute, Executive order, regulation, or other lawful order specifically imposes a duty on the individual to provide the information sought, and the individual is subject to a penalty if he or she fails to provide the requested information. If providing the information is only a condition of or prerequisite to granting a benefit or privilege and the individual has the option of requesting the benefit or privilege, providing the information is always voluntary. However, the loss or denial of the privilege, benefit, or entitlement sought may be listed as a consequence of not furnishing the requested information.

B. FORMS

1. DoD forms

a. DoD Directive 5000.21 (reference (i)) provides guidance for preparing Privacy Act Statements for use with forms (see also paragraph B.1.b. of this Chapter).

b. When forms are used to collect personal information, the Privacy Act Statement shall appear as follows (listed in the order of preference):

(1) In the body of the form, preferably just below the title so that the reader will be advised of the contents of the statement before he or she begins to complete the form;

(2) On the reverse side of the form with an appropriate annotation under the title giving its location;

(3) On a tear-off sheet attached to the form; or

(4) As a separate supplement to the form.

2. Forms issued by non-DoD activities

a. Forms subject to the Privacy Act issued by other federal agencies have a Privacy Act Statement attached or included. Always ensure that the statement prepared by the originating agency is adequate for the purpose for which the form will be used by the DoD activity. If the Privacy Act Statement

provided is inadequate, the DoD Component concerned shall prepare a new statement or a supplement to the existing statement before using the form.

b. Forms issued by agencies not subject to the Privacy Act (state, municipal, and other local agencies) do not contain Privacy Act Statements. Before using a form prepared by such agencies to collect personal data subject to this Regulation, an appropriate Privacy Act Statement must be added.

CHAPTER 3

ACCESS BY INDIVIDUALS

A. INDIVIDUAL ACCESS TO PERSONAL INFORMATION

1. Individual access

a. The access provisions of this Regulation are intended for use by individuals about whom records are maintained in systems of records. Release of personal information to individuals under this Regulation is not considered public release of information.

b. Make available to the individual to whom the record pertains all of the personal information that can be released consistent with DoD responsibilities.

2. Individual requests for access

Individuals shall address requests for access to personal information in a system of records to the system manager or to the office designated in the DoD Component rules or the system notice.

3. Verification of identity

a. Before granting access to personal data, an individual may be required to provide reasonable verification of his or her identity.

b. Identity verification procedures shall not:

(1) Be so complicated as to discourage unnecessarily individuals from seeking access to information about themselves; or

(2) Be required of an individual seeking access to records which normally would be available under DoD 5400.7-R (reference (f)).

c. Normally, when individuals seek personal access to records pertaining to themselves, identification is made from documents that normally are readily available, such as employee and military identification cards, driver's license, other licenses, permits or passes used for routine identification purposes.

d. When access is requested by mail, identity verification may consist of the individual providing certain minimum identifying data, such as full name, date and place of birth, or such other personal information necessary to locate the record sought. If the information sought is of a sensitive nature, additional identifying data may be required. If notarization of requests is required, procedures shall be established for an alternate method of verification for individuals who do not have access to notary services, such as military members overseas.

e. If an individual wishes to be accompanied by a third party when seeking access to his or her records or to have the records released directly

to a third party, the individual may be required to furnish a signed access authorization granting the third party access.

f. An individual shall not be refused access to his or her record solely because he or she refuses to divulge his or her SSN unless the SSN is the only method by which retrieval can be made. (See subsection A.2. of Chapter 2).

g. The individual is not required to explain or justify his or her need for access to any record under this Regulation.

h. Only a denial authority may deny access and the denial must be in writing and contain the information required by subsection B.2. of this Chapter.

4. Granting individual access to records

a. Grant the individual access to the original record or an exact copy of the original record without any changes or deletions, except when changes or deletions have been made in accordance with subsection A.5. of Chapter 5. For the purpose of granting access, a record that has been amended under subsection C.2. of this Chapter is considered to be the original. See subsection A.5. of this Chapter for the policy regarding the use of summaries and extracts.

b. Provide exact copies of the record when furnishing the individual copies of records under this Regulation.

c. Explain in terms understood by the requestor any record or portion of a record that is not clear.

5. Illegible, incomplete, or partially exempt records

a. Do not deny an individual access to a record or a copy of a record solely because the physical condition or format of the record does not make it readily available (for example, deteriorated state or on magnetic tape). Either prepare an extract or recopy the document exactly.

b. If a portion of the record contains information that is exempt from access, an extract or summary containing all of the information in the record that is releasable shall be prepared.

c. When the physical condition of the record or its state makes it necessary to prepare an extract for release, ensure that the extract can be understood by the requester.

d. Explain to the requester all deletions or changes to the records.

6. Access to medical records

a. Disclose medical records to the individual to whom they pertain, even if a minor, unless a judgment is made that access to such records could have an adverse effect on the mental or physical health of the individual. Normally, this determination shall be made in consultation with a medical doctor.

b. If it is determined that the release of the medical information may be harmful to the mental or physical health of the individual:

(1) Send the record to a physician named by the individual; and

(2) In the transmittal letter to the physician explain why access by the individual without proper professional supervision could be harmful (unless it is obvious from the record).

c. Do not require the physician to request the records for the individual.

d. If the individual refuses or fails to designate a physician, the record shall not be provided. Such refusal of access is not considered a denial for Privacy Act reporting purposes. (See subsection B.1. of this Chapter).

e. Access to a minor's medical records may be granted to his or her parents or legal guardians. However, observe the following procedures:

(1) In the United States, the laws of the particular state in which the records are located may afford special protection to certain types of medical records (for example, records dealing with treatment for drug or alcohol abuse and certain psychiatric records). Even if the records are maintained by a military medical facilities these statutes may apply.

(2) For the purposes of parental access to the medical records and medical determinations regarding minors at overseas installation the age of majority is 18 years except when:

(a) A minor at the time he or she sought or consented to the treatment was between 15 and 17 years of age;

(b) The treatment was sought in a program which was authorized by regulation or statute to offer confidentiality of treatment records as a part of the program;

(c) The minor specifically requested or indicated that he or she wished the treatment record to be handled with confidence and not released to a parent or guardian; and

(d) The parent or guardian seeking access does not have the written authorization of the minor or a valid court order granting access.

(3) If all four of the above conditions are met, the parent or guardian shall be denied access to the medical records of the minor. Do not use these procedures to deny the minor access to his or her own records under this Regulation or any other statutes.

f. All members of the Military Services and all married persons are not considered minors regardless of age, and the parents of these individual do not have access to their medical records without written consent of the individual.

7. Access to information compiled in anticipation of civil action

a. An individual is not entitled under this Regulation to gain access to information compiled in reasonable anticipation of a civil action or proceeding.

b. The term "civil proceeding" is intended to include quasi-judicial and pretrial judicial proceedings that are the necessary preliminary steps to formal litigation.

c. Attorney work products prepared in conjunction with quasi-judicial, pretrial, and trial proceedings, to include those prepared to advise DoD Component officials of the possible legal consequences of a given course of action, are protected.

8. Access to investigatory records

a. Requests by individuals for access to investigatory records pertaining to themselves and compiled for law enforcement purposes are processed under this Regulation or DoD 5400.7-R (reference (f)) depending on which regulation gives them the greatest degree of access.

b. Process requests by individuals for access to investigatory record pertaining to themselves compiled for law enforcement purposes and in the custody of law enforcement activities that have been incorporated into systems of records exempted from the access provisions of this Regulation in accordance with section B. of Chapter 5 under reference (f). Do not deny an individual access to the record solely because it is in the exempt system, but give him or her automatically the same access he or she would receive under reference (f) (see also subsection A.10. of this Chapter).

c. Process requests by individuals for access to investigatory records pertaining to themselves that are in records systems exempted from access provisions under subsection C.1. of Chapter 5, under this Regulation, or reference (f) depending upon which regulation gives the greatest degree of access (see also subsection A.10. of this Chapter).

d. Refer individual requests for access to investigatory records exempted from access under section B. of Chapter 5 temporarily in the hands of a noninvestigatory element for adjudicative or personnel actions to the originating investigating agency. Inform the requester in writing of these referrals.

9. Nonagency records

a. Certain documents under the physical control of DoD personnel and used to assist them in performing official functions, are not considered "agency records" within the meaning of this Regulation. Uncirculated personal notes and records that are not disseminated or circulated to any person or organization (for example, personal telephone lists or memory aids) that are retained or discarded at the author's discretion and over which the Component exercises no direct control, are not considered agency records. However, if personnel are

officially directed or encouraged, either in writing or orally, to maintain such records, they may become "agency records," and may be subject to this Regulation.

b. The personal uncirculated handwritten notes of unit leaders, office supervisors, or military supervisory personnel concerning subordinates are not systems of records within the meaning of this Regulation. Such notes are an extension of the individual's memory. These notes, however, must be maintained and discarded at the discretion of the individual supervisor and not circulated to others. Any established requirement to maintain such notes (such as, written or oral directives, regulations, or command policy) make these notes "agency records" and they then must be made a part of a system of records. If the notes are circulated, they must be made a part of a system of records. Any action that gives personal notes the appearance of official agency records is prohibited, unless the notes have been incorporated into a system of records.

10. Relationship between the Privacy Act and the Freedom of Information Act

a. Process requests for individual access as follows:

(1) Requests by individuals for access to record pertaining to themselves made under the Freedom of Information Act (reference (i)) or DoD 5400.7-R (reference (f)) or DoD Component instructions implementing reference (f) are processed under the provisions of that reference.

(2) Requests by individuals for access to records pertaining to themselves made under the Privacy Act of 1972 (reference (b)), this Regulation, or the DoD Component instructions implementing this Regulation are processed under this Regulation.

(3) Requests by individuals for access to records about themselves that cite both Acts or the implementing regulations and instructions for both Acts are processed under this Regulation except:

(a) When the access provisions of reference (f) provide a greater degree of access; or

(b) When access to the information sought is controlled by another federal statute.

(c) If the former applies, follow the provisions of reference (f); and if the latter applies, follow the access procedures established under the controlling statute.

(4) Requests by individuals for access to information about themselves in systems of records that do not cite either Act or the implementing regulations or instructions for either Act are processed under the procedures established by this Regulation. However, there is no requirement to cite the specific provisions of this Regulation or the Privacy Act (reference (b)) when responding to such requests. Do not count these requests as Privacy Act request for reporting purposes (see Chapter 8).

b. Do not deny individuals access to personal information concerning themselves that would otherwise be releasable to them under either Act solely

because they fail to cite either Act or cite the wrong Act, regulation, or instruction.

c. Explain to the requester which Act or procedures have been used when granting or denying access under either Act (see also subparagraph A.10. a.(4) of this Chapter).

11. Time limits. Normally acknowledge requests for access within 10 working days after receipt and provide access within 30 working days.

12. Privacy case file. Establish a Privacy Act case file when required (see subsection C.16. of this Chapter).

B. DENIAL OF INDIVIDUAL ACCESS

1. Denying individual access

a. An individual may be denied formally access to a record pertaining to him or her only if the record:

(1) Was compiled in reasonable anticipation of civil action (see subsection A.7. of this Chapter.)

(2) Is in a system of records that has been exempted from the access provisions of this Regulation under one of the permitted exemptions (see Chapter 5).

(3) Contains classified information that has been exempted from the access provision of this Regulation under the blanket exemption for such material claimed for all DoD records systems (see subsection A.3. of Chapter 5).

(4) Is contained in a system of records for which access may be denied under some other federal statute.

b. Only deny the individual access to those portions of the records from which the denial of access serves some legitimate governmental purpose.

2. Other reasons to refuse access

a. An individual may be refused access if:

(1) The record is not described well enough to enable it to be located with a reasonable amount of effort on the part of an employee familiar with the file; or

(2) Access is sought by an individual who fails or refuses to comply with the established procedural requirements, including refusing to name a physician to receive medical records when required (see subsection A.6. of this Chapter) or to pay fees (see section D. of this Chapter).

b. Always explain to the individual the specific reason access has been refused and how he or she may obtain access.

3. Notifying the individual. Formal denials of access must be in writing and include as a minimum:

a. The name, title or position, and signature of a designated Component denial authority;

b. The date of the denial;

c. The specific reason for the denial, including specific citation to the appropriate sections of the Privacy Act or other statutes, this Regulation, DoD Component instructions or Code of Federal Regulations (CFR) authorizing the denial;

d. Notice to the individual of his or her right to appeal the denial through the Component appeal procedure within 60 calendar days; and

e. The title or position and address of the Privacy Act appeals official for the Component.

4. DoD Component appeal procedures. Establish internal appeal procedures that, as a minimum, provide for:

a. Review by the head of the Component or his or her designee of any appeal by an individual from a denial of access to Component records.

b. Formal written notification to the individual by the appeal authority that shall:

(1) If the denial is sustained totally or in part, include as a minimum:

(a) The exact reason for denying the appeal to include specific citation to the provisions of the Act or other statute, this Regulation, Component instructions or the CFR upon which the determination is based;

(b) The date of the appeal determination;

(c) The name, title, and signature of the appeal authority; and

(d) A statement informing the applicant of his or her right to seek judicial relief.

(2) If the appeal is granted, notify the individual and provide access to the material to which access has been granted.

c. The written appeal notification granting or denying access is the final Component action as regards access.

d. The individual shall file any appeals from denial of access within no less than 60 calendar days of receipt of the denial notification.

e. Process all appeals within 30 days of receipt unless the appeal authority determines that a fair and equitable review cannot be made within that period. Notify the applicant in writing if additional time is required for the appellate review. The notification must include the reasons for the delay and state when the individual may expect an answer to the appeal.

5. Denial of appeals by failure to act. A requester may consider his or her appeal formally denied if the appeal authority fails:

a. To act on the appeal within 30 days;

b. To provide the requester with a notice of extension within 30 days; or

c. To act within the time limits established in the Component's notice of extension (see paragraph B.4.e. of this Chapter).

6. Denying access to OPM records held by DoD Components

a. The records in all systems of records maintained in accordance with the OPM government-wide system notices are technically only in the temporary custody of the Department of Defense.

b. All requests for access to these records must be processed in accordance with the Federal Personnel Manual (reference (h)) as well as the applicable Component procedures.

c. When a DoD Component refuses to grant access to a record in an OPM system, the Component shall instruct the individual to direct his or her appeal to the appropriate Component appeal authority, not the Office of Personnel Management.

d. The Component is responsible for the administrative review of its denial of access to such records.

C. AMENDMENT OF RECORDS

1. Individual review and correction. Individuals are encouraged to review the personal information being maintained about them by DoD Components periodically and to avail themselves of the procedures established by this Regulation and other regulations to update their records.

2. Amending records

a. An individual may request the amendment of any record contained in a system of records pertaining to him or her unless the system of record has been exempted specifically from the amendment procedures of this Regulation under subsection A.2. of Chapter 5. Normally, amendments under this Regulation are limited to correcting factual matters and not matters of official judgment, such as performance ratings, promotion potential, and job performance appraisals.

b. While a Component may require that the request for amendment be in writing, this requirement shall not be used to discourage individuals from requesting valid amendments or to burden needlessly the amendment process.

c. A request for amendment must include:

(1) A description of the item or items to be amended;

(2) The specific reason for the amendment;

(3) The type of amendment action sought (deletion, correction, or addition); and

(4) Copies of available documentary evidence supporting the request.

3. Burden of proof. The applicant must support adequately his or her claim.

4. Identification of requesters

a. Individuals may be required to provide identification to ensure that they are indeed seeking to amend a record pertaining to themselves and not, inadvertently or intentionally, the record of others.

b. The identification procedures shall not be used to discourage legitimate requests or to burden needlessly or delay the amendment process. (See subsection A.3. of this Chapter.)

5. Limits on attacking evidence previously submitted

a. The amendment process is not intended to permit the alteration of evidence presented in the course of judicial or quasi-judicial proceedings. Any amendments or changes to these records normally are made through the specific procedures established for the amendment of such records.

b. Nothing in the amendment process is intended or designed to permit a collateral attack upon what has already been the subject of a judicial or quasi-judicial determination. However, while the individual may not attack the accuracy of the judicial or quasi-judicial determination under this Regulation, he or she may challenge the accuracy of the recording of that action.

6. Sufficiency of a request to amend. Consider the following factors when evaluating the sufficiency of a request to amend:

a. The accuracy of the information itself; and

b. The relevancy, timeliness, completeness, and necessity of the recorded information for accomplishing an assigned mission or purpose.

7. Time limits

a. Provide written acknowledgement of a request to amend within 10 working days of its receipt by the appropriate systems manager. There is no need to acknowledge a request if the action is completed within 10 working days and the individual is so informed.

b. The letter of acknowledgement shall clearly identify the request and advise the individual when he or she may expect to be notified of the completed action.

c. Only under the most exceptional circumstances shall more than 30 days be required to reach a decision on a request to amend. Document fully and explain in the Privacy Act case file (see subsection C.16. of this Chapter) any such decision that takes more than 30 days to resolve.

8. Agreement to amend. If the decision is made to grant all or part of the request for amendment, amend the record accordingly and notify the requester.

9. Notification of previous recipients

a. Notify all previous recipients of the information, as reflected in the disclosure accounting records, that an amendment has been made and the substance of the amendment. Recipients who are known to be no longer retaining the information need not be advised of the amendment. All DoD Components and federal agencies known to be retaining the record or information, even if not reflected in a disclosure record, shall be notified of the amendment. Advise the requester of these notifications.

b. Honor all requests by the requester to notify specific federal agencies of the amendment action.

10. Denying amendment. If the request for amendment is denied in whole or in part, promptly advise the individual in writing of the decision to include:

a. The specific reason and authority for not amending;

b. Notification that he or she may seek further independent review of the decision by the head of the Component or his or her designee;

c. The procedures for appealing the decision citing the position and address of the official to whom the appeal shall be addressed; and

d. Where he or she can receive assistance in filing the appeal.

11. DoD Component appeal procedures. Establish procedures to ensure the prompt, complete, and independent review of each amendment denial upon appeal by the individual. These procedures must ensure that:

a. The appeal with all supporting materials both that furnished the individual and that contained in Component records is provided to the reviewing official, and

b. If the appeal is denied completely or in part, the individual is notified in writing by the reviewing official that:

(1) The appeal has been denied and the specific reason and authority for the denial;

(2) The individual may file a statement of disagreement with the appropriate authority and the procedures for filing this statement;

(3) If filed properly, the statement of disagreement shall be included in the records, furnished to all future recipients of the records, and provided to all prior recipients of the disputed records who are known to hold the record; and

(4) The individual may seek a judicial review of the decision not to amend.

c. If the record is amended, ensure that:

(1) The requester is notified promptly of the decision;

(2) All prior known recipients of the records who are known to be retaining the record are notified of the decision and the specific nature of the amendment (see subsection C.9. of this Chapter); and

(3) The requester is notified as to which DoD Components and federal agencies have been told of the amendment.

d. Process all appeals within 30 days unless the appeal authority determines that a fair review cannot be made within this time limit. If additional time is required for the appeal, notify the requester, in writing, of the delay, the reason for the delay, and when he or she may expect a final decision on the appeal. Document fully all requirements for additional time in the Privacy Case File. (See subsection C.16. of this Chapter.)

12. Denying amendment of OPM records held by DoD Components

a. The records in all systems of records controlled by the Office of Personnel Management (OPM) government-wide system notices are technically only temporarily in the custody of the Department of Defense.

b. All requests for amendment of these records must be processed in accordance with the Federal Personnel Manual (reference (h)). The Component denial authority may deny a request. However, the appeal process for all such denials must include a review by the Assistant Director for Agency Compliance and Evaluation, Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415.

c. When an appeal is received from a Component's denial of amendment of the OPM controlled record, process the appeal in accordance with reference (h) and notify the OPM appeal authority listed above.

d. The individual may appeal any Component decision not to amend the OPM records directly to OPM.

e. OPM is the final review authority for any appeals from a denial to amend the OPM records.

13. Statements of disagreement submitted by individuals

a. If the reviewing authority refuses to amend the record as requested, the individual may submit a concise statement of disagreement setting forth his or her reasons for disagreeing with the decision not to amend.

b. If an individual chooses to file a statement of disagreement, annotate the record to indicate that the statement has been filed (see subsection C.14. of this Chapter).

c. Furnish copies of the statement of disagreement to all DoD Components and federal agencies that have been provided copies of the disputed information and who may be maintaining the information.

14. Maintaining statements of disagreement

a. When possible, incorporate the statement of disagreement into the record.

b. If the statement cannot be made a part of the record, establish procedures to ensure that it is apparent from the records that a statement of disagreement has been filed and maintain the statement so that it can be obtained readily when the disputed information is used or disclosed.

c. Automated record systems that are not programed to accept statements of disagreement shall be annotated or coded so that they clearly indicate that a statement of disagreement is on file, and clearly identify the statement with the disputed information in the system.

d. Provide a copy of the statement of disagreement whenever the disputed information is disclosed for any purpose.

15. DoD Component summaries of reasons for refusing to amend

a. A summary of reasons for refusing to amend may be included with any record for which a statement of disagreement is filed.

b. Include in this summary only the reasons furnished to the individual for not amending the record. Do not include comments on the statement of disagreement. Normally, the summary and statement of disagreement are filed together.

c. When disclosing information for which a summary has been filed, a copy of the summary may be included in the release, if the Component desires.

16. Privacy Case Files

a. Establish a separate Privacy Case File to retain the documentation received and generated during the amendment or access process.

b. The Privacy Case File shall contain as a minimum:

(1) The request for amendment or access;

(2) Copies of the DoD Component's reply granting or denying the request;

(3) Any appeals from the individual;

(4) Copies of the action regarding the appeal with supporting documentation which is not in the basic file; and

(5) Any other correspondence generated in processing the appeal, to include coordination documentation.

c. Only the items listed in paragraphs C.16.d. and e. of this Chapter may be included in the system of records challenged for amendment or for which access is sought. Do not retain copies of unamended records in the basic record system if the request for amendment is granted.

d. The following items relating to an amendment request may be included in the disputed record system:

(1) Copies of the amended record.

(2) Copies of the individual's statement of disagreement (see subsection C.13. of this Chapter).

(3) Copies of Component summaries (see subsection C.15. of this Chapter).

(4) Supporting documentation submitted by the individual.

e. The following items relating to an access request may be included in the basic records system:

(1) Copies of the request;

(2) Copies of the Component's action granting total access. (Note: A separate Privacy case file need not be created in such cases).

(3) Copies of the Component's action denying access;

(4) Copies of any appeals filed;

(5) Copies of the reply to the appeal.

f. There is no need to establish a Privacy case file if the individual has not cited the Privacy Act (reference (b)), this Regulation, or the Component implementing instruction for this Regulation.

g. Privacy case files shall not be furnished or disclosed to anyone for use in making any determination about the individual other than determinations made under this Regulation.

D. REPRODUCTION FEES

1. Assessing fees

a. Charge the individual only the direct cost of reproduction.

b. Do not charge reproduction fees if copying is:

(1) The only means to make the record available to the individual (for example, a copy of the record must be made to delete classified information); or

(2) For the convenience of the DoD Component (for example, the Component has no reading room where an individual may review the record, or reproduction is done to keep the original in the Component's file).

c. No fees shall be charged when the record may be obtained without charge under any other regulation, directive, or statute.

d. Do not use fees to discourage requests.

2. No minimum fees authorized. Use fees only to recoup direct reproduction costs associated with granting access. Minimum fees for duplication are not authorized and there is no automatic charge for processing a request.

3. Prohibited Fees. Do not charge or collect fees for:

a. Search and retrieval of records;

b. Review of records to determine releasability;

c. Copying records for DoD Component convenience or when the individual has not specifically requested a copy;

d. Transportation of records and personnel; or

e. Normal postage.

4. Waiver of Fees.

a. Normally, fees are waived automatically if the direct costs of a given request is less than $30. This fee waiver provision does not apply when a waiver has been granted to the individual before, and later requests appear to be an extension or duplication of that original request. A DoD Component may, however, set aside this automatic fee waiver provision when on the basis of good evidence it determines that the waiver of fees is not in the public interest.

b. Decisions to waiver or reduce fees that exceed the automatic waiver threshold shall be made on a case-by-case basis.

5. Fees for members of Congress. Do not charge members of Congress for copying records furnished even when the records are requested under the Privacy Act on behalf of a constituent (see subsection B.11. of Chapter 4). When replying to a constituent inquiry and the fees involved are substantial, consider suggesting to the Congressman that the constituent can obtain the information directly by writing to the appropriate offices and paying the costs. When practical, suggest to the Congressman that the record can be examined at no cost if the constituent wishes to visit the custodian of the record.

6. Reproduction fees computation. Compute fees using the appropriate portions of the fee schedule in DoD 5400.7-R (reference (f)).

CHAPTER 4

DISCLOSURE OF PERSONAL INFORMATION TO OTHER AGENCIES AND THIRD PARTIES

A. CONDITIONS OF DISCLOSURE

1. Disclosures to third parties

a. The Privacy Act only compels disclosure of records from a system of records to the individuals to whom they pertain.

b. All requests by individuals for personal information about other individuals (third parties) shall be processed under DoD 5400.7-R (reference (f)), except for requests by the parents of a minor, or legal guardians of an individual, for access to the records pertaining to the minor or individual.

2. Disclosures among DoD Components. For the purposes of disclosure and disclosure accounting, the Department of Defense is considered a single agency (see subsection B.1. of this Chapter).

3. Disclosures outside the Department of Defense. Do not disclose personal information from a system of records outside the Department of Defense unless:

a. The record has been requested by the individual to whom it pertains.

b. The written consent of the individual to whom the record pertains has been obtained for release of the record to the requesting agency, activity, or individual, or

c. The release is for one of the specific nonconsensual purposes set forth in section B. of this Chapter.

4. Validation before disclosure. Except for releases made in accordance with reference (f), before disclosing any personal information to any recipient outside the Department of Defense other than a federal agency or the individual to whom it pertains:

a. Ensure that the records are accurate, timely, complete, and relevant for agency purposes;

b. Contact the individual, if reasonably available, to verify the accuracy, timeliness, completeness, and relevancy of the information, if this cannot be determined from the record; or

c. If the information is not current and the individual is not reasonably available, advise the recipient that the information is believed accurate as of a specific date and any other known factors bearing on its accuracy and relevancy.

B. NONCONSENSUAL DISCLOSURES

1. Disclosures within the Department of Defense

a. Records pertaining to an individual may be disclosed without the consent of the individual to any DoD official who has need for the record in the performance of his or her assigned duties.

b. Rank, position, or title alone do not authorize access to personal information about others. An official need for the information must exist before disclosure.

2. Disclosures under DoD 5400.7-R (reference (f))

a. All records must be disclosed if their release is required by the Freedom of Information Act (reference (j), see also reference (f)). Reference (j) requires that records be made available to the public unless exempted from disclosure by one of the nine exemptions found in the Act. It follows, therefore, that if a record is not exempt from disclosure it must be disclosed.

b. The standard for exempting most personal records, such as personnel records, medical records, and similar records, is found in Exemption Number 6 of paragraph 3-200, reference (f). Under that exemption, release of personal information can only be denied when its release would be a "clearly unwarranted invasion of personal privacy."

c. Release of personal information in investigatory records including personnel security investigation records is controlled by the broader standard of an "unwarranted invasion of personal privacy" found in Exemption Number 7 of paragraph 3-200, reference (f). This broader standard applies only to investigatory records.

d. See reference (f) for the standards to use in applying these exemptions.

3. Personal information that is normally releasable

a. DoD civilian employees

(1) Some examples of personal information regarding DoD civilian employees that normally may be released without a clearly unwarranted invasion of personal privacy include:

(a) Name.

(b) Present and past position titles.

(c) Present and past grades.

(d) Present and past salaries.

(e) Present and past duty stations.

(f) Office or duty telephone numbers.

(2) All disclosures of personal information regarding federal civilian employees shall be made in accordance with the Federal Personnel Manual (FPM) (reference (h)).

b. Military members

(1) While it is not possible to identify categorically information that must be released or withheld from military personnel records in every instance, the following items of personal information regarding military members normally may be disclosed without a clearly unwarranted invasion of their personal privacy:

(a) Full name.

(b) Rank.

(c) Date of rank.

(d) Gross salary.

(e) Past duty assignments.

(f) Present duty assignment.

(g) Future assignments that are officially established.

(h) Office or duty telephone numbers.

(i) Source of commission.

(j) Promotion sequence number.

(k) Awards and decorations.

(l) Attendance at professional military schools.

(m) Duty status at any given time.

(2) All releases of personal information regarding military members shall be made in accordance with the standards established by DoD 5400.7-R (reference (f)).

c. Civilian employees not under the FPM

(1) While it is not possible to identify categorically those items of personal information that must be released regarding civilian employees not subject to reference (h), such as nonappropriated fund employees, normally the following items may be released without a clearly unwarranted invasion of personal privacy:

(a) Full name.

(b) Grade or position.

(c) Date of grade.

(d) Gross salary.

(e) Present and past assignments.

(f) Future assignments, if officially established.

(g) Office or duty telephone numbers.

(2) All releases of personal information regarding civilian personnel in this category shall be made in accordance with the standards established by DoD 5400.7-R (reference (f)).

4. Release of home addresses and home telephone numbers

a. The release of home addresses and home telephone numbers normally is considered a clearly unwarranted invasion of personal privacy and is prohibited. However, these may be released without prior specific consent of the individual if:

(1) The individual has indicated previously that he or she interposes no objection to their release (see paragraphs B.4.c. and d. of this Chapter);

(2) The source of the information to be released is a public document such as commercial telephone directory or other public listing;

(3) The release is required by federal statute (for example, pursuant to federally-funded state programs to locate parents who have defaulted on child support payments (42 U.S.C. Section 653, reference (k)); or

(4) The releasing official releases the information under the provisions of DoD 5400.7-R (reference (f)).

b. A request for a home address or telephone number may be referred to the last known address of the individual for a direct reply by him or her to the requester. In such cases the requester shall be notified of the referral.

c. When collecting lists of home addresses and telephone numbers, the individual may be offered the option of authorizing the information pertaining to him or her to be disseminated without further permission for specific purposes, such as locator services. In these cases, the information may be disseminated for the stated purpose without further consent. However, if the information is to be disseminated for any other purpose, a new consent is required. Normally such consent for release is in writing and signed by the individual.

d. Before listing home addresses and home telephone numbers in DoD telephone directories, give the individuals the opportunity to refuse such a listing. Excuse the individual from paying any additional cost that may be associated with maintaining an unlisted number for government-owned telephone services if the individual requests his or her number not be listed in the directory under this Regulation.

e. Do not sell or rent lists of individual names and addresses unless such action is specifically authorized.

5. Disclosures for established routine uses

a. Records may be disclosed outside the Department of Defense without consent of the individual to whom they pertain for an established routine use.

b. A routine use shall:

(1) Be compatible with and related to the purpose for which the record was compiled;

(2) Identify the persons or organizations to whom the record may be released;

(3) Identify specifically the uses to which the information may be put by the receiving agency; and

(4) Have been published previously in the Federal Register (see subsection C.9. of Chapter 6).

c. Establish a routine use for each user of the information outside the Department of Defense who need official access to the records.

d. Routine uses may be established, discontinued, or amended without the consent of the individuals involved. However, new or changed routine uses must be published in the Federal Register at least 30 days before actually disclosing any records under their provisions (see Chapter 6).

e. In addition to the routine uses established by the individual system notices, common blanket routine uses for all DoD-maintained systems of records have been established (see Appendix C). These blanket routine uses are published only at the beginning of the listing of system notices for each Component in the Federal Register (see subsection D.3. of Chapter 6). Unless a system notice specifically excludes a system from a given blanket routine use, all blanket routine uses apply.

f. If the recipient has not been identified in the Federal Register or a use to which the recipient intends to put the record has not been published in the system notice as a routine use, the written permission of the individual is required before release or use of the record for that purpose.

6. Disclosures to the Bureau of the Census

Records in DoD systems of records may be disclosed without the consent of the individuals to whom they pertain to the Bureau of the Census for purposes of planning or carrying out a census survey or related activities pursuant to the provisions of 13 U.S.C., section 8 (reference (l)).

7. Disclosures for statistical research and reporting

a. Records may be disclosed for statistical research and reporting without the consent of the individuals to whom they pertain. Before such disclosures the recipient must provide advance written assurance that:

(1) The records will be used as statistical research or reporting records;

(2) The records will only be transferred in a form that is not individually identifiable; and

(3) The records will not be used, in whole or in part, to make any determination about the rights, benefits, or entitlements of specific individuals.

b. A disclosure accounting (see subsection E.1. of this Chapter) is not required when information that is not identifiable individually is released for statistical research or reporting.

8. Disclosures to the National Archives and Record Service (NARS), General Services Administration

a. Records may be disclosed without the consent of the individual to whom they pertain to the NARS if they:

(1) Have historical or other value to warrant continued preservation; or

(2) For evaluation by the NARS to determine if a record has such historical or other value.

b. Records transferred to a Federal Records Center (FRC) for safekeeping and storage do not fall within this category. These remain under the control of the transferring Component, and the FRC personnel are considered agents of the Component which retains control over the records. No disclosure accounting is required for the transfer of records to the FRCs.

9. Disclosures for law enforcement purposes

a. Records may be disclosed without the consent of the individual to whom they pertain to another agency or an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, provided:

(1) The civil or criminal law enforcement activity is authorized by law;

(2) The head of the law enforcement activity or a designee has made a written request specifying the particular records desired and the law enforcement purpose (such as criminal investigations, enforcement of a civil law, or a similar purpose) for which the record is sought; and

(3) There is no federal statute that prohibits the disclosure of the records.

b. Normally, blanket requests for access to any and all records pertaining to an individual are not honored.

c. When a record is released to a law enforcement activity under paragraph B.10.a. of this Chapter, maintain a disclosure accounting. This disclosure accounting shall not be made available to the individual to whom the record pertains if the law enforcement activity requests that the disclosure not be released.

d. The blanket routine use for Law Enforcement (Appendix C, section A.) applies to all DoD Component systems notices (see paragraph B.5.e. of this Chapter). Only by including this routine use can a Component, on its own initiative, report indications of violations of law found in a system of records to a law enforcement activity without the consent of the individual to whom the record pertains (see paragraph B.9.a. of this Chapter when responding to requests from law enforcement activities).

10. Emergency disclosures

a. Records may be disclosed without the consent of the individual to whom they pertain if disclosure is made under compelling circumstances affecting the health or safety of any individual. The affected individual need not be the subject of the record disclosed.

b. When such a disclosure is made, notify the individual who is the subject of the record. Notification sent to the last known address of the individual as reflected in the records is sufficient.

c. The specific data to be disclosed is at the discretion of releasing authority.

d. Emergency medical information may be released by telephone.

11. Disclosures to Congress and the General Accounting Office

a. Records may be disclosed without the consent of the individual to whom they pertain to either House of the Congress or to any committee, joint committee or subcommittee of Congress if the release pertains to a matter within the jurisdiction of the committee. Records may also be disclosed to the General Accounting Office (GAO) in the course of the activities of GAO.

b. The blanket routine use for "Congressional Inquiries" (see Appendix C, section D.) applies to all systems; therefore, there is no need to verify that the individual has authorized the release of his or her record to a congressional member when responding to a congressional constituent inquiry.

c. If necessary, accept constituent letters requesting a member of Congress to investigate a matter pertaining to the individual as written authorization to provide access to the records to the congressional member or his or her staff.

d. The verbal statement by a congressional staff member is acceptable to establish that a request has been received from the person to whom the records pertain.

e. If the constituent inquiry is being made on behalf of someone other than the individual to whom the record pertains, provide the congressional member only that information releasable under DoD 5400.7-R (reference (f)). Advise the congressional member that the written consent of the individual to whom the record pertains is required before any additional information may be released. Do not contact individuals to obtain their consents for release to congressional members unless a congressional office specifically requests that this be done.

f. Nothing in paragraph B.11.b. of this Chapter prohibits a Component, when appropriate, from providing the record directly to the individual and notifying the congressional office that this has been done without providing the record to the congressional member.

g. See subsection D.5. of Chapter 3 for the policy on assessing fees for Members of Congress.

h. Make a disclosure accounting each time a record is disclosed to either House of Congress, to any committee, joint committee, or subcommittee of Congress, to any congressional member, or GAO.

12. Disclosures under court orders

a. Records may be disclosed without the consent of the person to whom they pertain under a court order signed by a judge of a court of competent jurisdiction. Releases may also be made under the compulsory legal process of federal or state bodies having authority to issue such process.

b. When a record is disclosed under this provision, make reasonable efforts to notify the individual to whom the record pertains, if the legal process is a matter of public record.

c. If the process is not a matter of public record at the time it is issued, seek to be advised when the process is made public and make reasonable efforts to notify the individual at that time.

d. Notification sent to the last known address of the individual as reflected in the records is considered reasonable effort to notify.

e. Make a disclosure accounting each time a record is disclosed under a court order or compulsory legal process.

13. Disclosures to consumer reporting agencies

a. Certain personal information may be disclosed to consumer reporting agencies as defined by the Federal Claims Collection Act of 1966, as amended (reference (e)).

b. Under the provisions of reference (e) the following information may be disclosed to a consumer reporting agency:

(1) Name, address, taxpayer identification number (SSN), and other information necessary to establish the identity of the individual.

(2) The amount, status, and history of the claim.

(3) The agency or program under which the claim arose.

c. Reference (e) specifically requires that the system notice for the system of records from which the information will be disclosed indicates that the information may be disclosed to a consumer reporting agency.

C. DISCLOSURES TO COMMERCIAL ENTERPRISES

1. General policy

a. Make releases of personal information to commercial enterprises under the criteria established by DoD 5400.7-R (reference (f)).

b. The relationship of commercial enterprises to their clients or customers and to the Department of Defense are not changed by this Regulation.

c. The DoD policy on personal indebtedness for military personnel is contained in DoD Directive 1344.9 (reference (m)) and for civilian employees in the FPM (reference (h)).

2. Release of personal information

a. Any information that must be released under reference (f) may be released to a commercial enterprise without the individual's consent (see subsection B.2. of this Chapter).

b. Commercial enterprises may present a signed consent statement setting forth specific conditions for release of personal information. Statements such as the following, if signed by the individual, are considered valid:

> "I hereby authorize the Department of Defense to verify my Social Security Number or other identifying information and to disclose my home address and telephone number to authorized representatives of (name of commercial enterprise) so that they may use this information in connection with my commercial dealings with that enterprise. All information furnished will be used in connection with my financial relationship with (name of commercial enterprise)."

c. When a statement of consent as outlined in paragraph C.2.b. of this Chapter is presented, provide the requested information if its release is not prohibited by some other regulation or statute.

d. Blanket statements of consent that do not identify specifically the Department of Defense or any of its Components, or that do not specify exactly the type of information to be released, may be honored if it is clear that the individual in signing the consent statement intended to obtain a personal benefit (for example, a loan to buy a house) and was aware of the type information that would be sought. Care should be exercised in these situations to release only the minimum amount of personal information essential to obtain the benefit sought.

e. Do not honor requests from commercial enterprises for official evaluation of personal characteristics, such as evaluation of personal financial habits.

D. DISCLOSURES TO THE PUBLIC FROM HEALTH CARE RECORDS

1. Section applicability. This section applies to the release of information to the news media or the public concerning persons treated or hospitalized in DoD medical facilities and patients of nonfederal medical facilities for whom the cost of the care is paid by the Department of Defense.

2. General disclosure. Normally, the following may be released without the patient's consent.

a. Personal information concerning the patient. See DoD 5400.7-R (reference (f)) and subsection B.3. of this Chapter.

b. Medical condition:

(1) Date of admission or disposition;

(2) The present medical assessment of the individual's condition in the following terms if the medical doctor has volunteered the information:

(a) The individual's condition is presently (stable) (good) (fair) (serious) or (critical), and

(b) Whether the patient is conscious, semiconscious, or unconscious.

3. Individual consent

a. Detailed medical and other personal information may be released in response to inquiries from the news media and public if the patient has given his or her informed consent to such a release.

b. If the patient is not conscious or competent, no personal information except that required by reference (f) shall be released until there has been enough improvement in the patient to ensure he or she can give informed consent or a guardian has been appointed legally for the patient and the guardian has given consent on behalf of the patient.

c. The consent described in paragraph D.3.a. of this Chapter regarding patients who are minors must be given by the parent or legal guardian.

4. Information that may be released with individual consent

a. Any item of personal information may be released, if the patient has given his or her informed consent to its release.

b. Releasing medical information about patients shall be done with discretion, so as not to embarrass the patient, his or her family, or the Department of Defense, needlessly.

5. Disclosures to other government agencies. This Chapter does not limit the disclosures of personal medical information to other government agencies for use in determining eligibility for special assistance or other benefits.

E. DISCLOSURE ACCOUNTING

1. Disclosure accountings

a. Keep an accurate record of all disclosures made from any system of records except disclosures:

(1) To DoD personnel for use in the performance of their official duties; or

(2) Under DoD 5400.7-R (reference (f)).

b. In all other cases a disclosure accounting is required even if the individual has consented to the disclosure of the information pertaining to him or her.

c. Disclosure accountings:

(1) Permit individuals to determine to whom information has been disclosed;

(2) Enable the activity to notify past recipients of disputed or corrected information (subsections C.9. of Chapter 3); and

(3) Provide a method of determining compliance with subsection A.3. of this Chapter.

2. Contents of disclosure accountings. As a minimum, disclosure accounting shall contain:

a. The date of the disclosure.

b. A description of the information released.

c. The purpose of the disclosure.

d. The name and address of the person or agency to whom the disclosure was made.

3. Methods of disclosure accounting. Use any system of disclosure accounting that will provide readily the necessary disclosure information (see paragraph E.1.c. of this Chapter).

4. Accounting for mass disclosures. When numerous similar records are released (such as transmittal of payroll checks to a bank), identify the

category of records disclosed and include the data required by subsection E.2. of this Chapter in some form that can be used to construct an accounting disclosure record for individual records if required (see paragraph E.1.c. of this Chapter).

5. Disposition of disclosure accounting records. Retain disclosure accounting records for 5 years after the disclosure or the life of the record, whichever is longer.

6. Furnishing disclosure accountings to the individual

a. Make available to the individual to whom the record pertains all disclosure accountings except when:

(1) The disclosure has been made to a law enforcement activity under subsection B.9. of this Chapter and the law enforcement activity has requested that disclosure not be made; or

(2) The system of records has been exempted from the requirement to furnish the disclosure accounting under the provisions of subsection A.2. of Chapter 5.

b. If disclosure accountings are not maintained with the record and the individual requests access to the accounting, prepare a listing of all disclosures (see subsection E.2. this Chapter) and provide this to the individual upon request.

CHAPTER 5

EXEMPTIONS

A. USE AND ESTABLISHMENT OF EXEMPTIONS

1. Types of exemptions

a. There are two types of exemptions permitted by the Privacy Act.

(1) General exemptions that authorize the exemption of a system of records from all but certain specifically identified provisions of the Act.

(2) Specific exemptions that allow a system of records to be exempted only from certain designated provisions of the Act.

b. Nothing in the Act permits exemption of any system of records from all provisions of the Act.

2. Establishing exemptions

a. Neither general nor specific exemptions are established automatically for any system of records. The head of the DoD Component maintaining the system of records must make a determination whether the system is one for which an exemption properly may be claimed and then propose and establish an exemption rule for the system. No system of records within the Department of Defense shall be considered exempted until the head of the Component has approved the exemption and an exemption rule has been published as a final rule in the Federal Register (see subsection A.6. of Chapter 6).

b. Only the head of the DoD Component or an authorized designee may claim an exemption for a system of records.

c. A system of records is considered exempt only from those provision of the Privacy Act (reference (b)) which are identified specifically in the Component exemption rule for the system and which are authorized by reference (b).

d. To establish an exemption rule, see subsection B.2. of Chapter 6.

3. Blanket exemption for classified material

a. Include in the Component rules a blanket exemption under 5 U.S.C. 552a(k)(1) (reference (b)) from the access provisions (5 U.S.C. 552a(d)) and the notification of access procedures (5 U.S.C. 522a(e)(4)(H)) of the Act for all classified material in any systems of records maintained.

b. Do not claim specifically an exemption under section 552a(k)(1) (reference (b)) for any system of records. The blanket exemption affords protection to all classified material in all system of records maintained.

4. Provisions from which exemptions may be claimed

a. The head of a DoD Component may claim an exemption from any provision of the Act from which an exemption is allowed (see Appendix D).

b. Notify the Defense Privacy Office before claiming an exemption for any system of records from the following:

(1) The exemption rule publication requirement (5 U.S.C. 552a(j)) (reference (b));

(2) The requirement to report new systems of records (5 U.S.C. 552a(o)); or

(3) The annual report requirement (5 U.S.C. 552a(p)).

5. Use of exemptions

a. Use exemptions only for the specific purposes set forth in the exemption rules (see subsection B.2. of Chapter 6).

b. Use exemptions only when they are in the best interest of the government and limit them to the specific portions of the records requiring protection.

c. Do not use an exemption to deny an individual access to any record to which he or she would have access under DoD 5200.7-R (reference (f)).

6. Exempt records in nonexempt systems

a. Exempt records temporarily in the hands of another Component are considered the property of the originating Component and access to these records is controlled by the system notices and rules of the originating Component.

b. Records that are actually incorporated into a system of records may be exempted only to the extent the system of records into which they are incorporated has been granted an exemption, regardless of their original status or the system of records for which they were created.

c. If a record is accidentally misfiled into a system of records, the system notice and rules for the system in which it should actually be filed will govern.

B. GENERAL EXEMPTIONS

1. Use of the general exemptions

a. No DoD Component is authorized to claim the exemption for records maintained by the Central Intelligence Agency established by 5 U.S.C. 552a(j)(1) (reference (b)).

b. The general exemption established by 5 U.S.C. 552a(j)(2) (reference (b)) may be claimed to protect investigative records created and maintained by law-enforcement activities of a DoD Component.

c. To qualify for the (j)(2) exemption, the system of records must be maintained by an element that performs as its principal function enforcement of the criminal law, such as U.S. Army Criminal Investigation Command (CIDC), Naval Investigative Service (NIS), the Air Force Office of Special Investigations (AFOSI), and military police activities. Law enforcement includes police efforts to detect, prevent, control, or reduce crime, to apprehend or identify criminals; and the activities of correction, probation, pardon, or parole authorities.

d. Information that may be protected under the (j)(2) exemption include:

(1) Records compiled for the purpose of identifying criminal offenders and alleged offenders consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, parole, and probation status (so-called criminal history records);

(2) Reports and other records compiled during criminal investigations, to include supporting documentation.

(3) Other records compiled at any stage of the criminal law enforcement process from arrest or indictment through the final release from parole supervision, such as presentence and parole reports.

e. The (j)(2) exemption does not apply to:

(1) Investigative records prepared or maintained by activities without primary law-enforcement missions. It may not be claimed by any activity that does not have law enforcement as its principal function.

(2) Investigative records compiled by any activity concerning employee suitability, eligibility, qualification, or for individual access to classified material regardless of the principal mission of the compiling DoD Component.

g. The (j)(2) exemption claimed by the law-enforcement activity will not protect investigative records that are incorporated into the record system of a nonlaw enforcement activity or into nonexempt systems of records (see paragraph A.6.b. of this Chapter). Therefore, all system managers are cautioned to comply with the various regulations prohibiting or limiting the incorporation of investigatory records into system of records other than those maintained by law-enforcement activities.

2. Access to records for which a (j)(2) exemption is claimed. Access to investigative records in the hands of a law-enforcement activity or temporarily in the hands of a military commander or other criminal adjudicative activity shall be processed under DoD 5200.7-R, (reference (f)) provided that the system of records from which the file originated is a law enforcement record system that has been exempted from the access provisions of this Regulation (see paragraph A.6.a. of Chapter 3).

C. SPECIFIC EXEMPTIONS

1. Use of the specific exemptions. The specific exemptions permit certain categories of records to be exempted from certain specific provisions of the Privacy Act (see Appendix D). To establish a specific exemption, the records must meet the following criteria (parenthetical references are to the appropriate subsection of the Act (5 U.S.C. 552a(k)) (reference (b)):

a. (k)(1). Information specifically authorized to be classified under DoD 5200.1-R (reference (a)) (see also subsection A.3. of this Chapter).

b. (k)(2). Investigatory information compiled for law-enforcement purposes by nonlaw enforcement activities and which is not within the scope of subsection B.1. of this Chapter. If an individual is denied any right, privilege or benefit that he or she is otherwise entitled by federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. This subsection when claimed allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

c. (k)(3). Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C., Section 3506 (reference (n)).

d. (k)(4). Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C., Section 8 (reference (l)).

e. (k)(5). Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source. This provision allows protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

f. (k)(6). Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.

g. (k)(7). Evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

2. Promises of confidentiality

a. Only the identity of sources that have been given an express promise of confidentiality may be protected from disclosure under paragraphs C.1.b., C.1.e., and C.1.g. However, the identity of sources who were given implied

promises of confidentiality in inquiries conducted before September 27, 1975, may also be protected from disclosure.

b. Ensure that promises of confidentiality are used on a limited basis in day-to-day operations. Establish appropriate procedures and identify fully those categories of individuals who may make such promises. Promises of confidentiality shall be made only when they are essential to obtain the information sought.

3. Access to records for which specific exemptions are claimed. Deny the individual access only to those portions of the records for which the claimed exemption applies.

CHAPTER 6

PUBLICATION REQUIREMENTS

A. FEDERAL REGISTER PUBLICATION

1. What must be published in the Federal Register

a. Three types of documents relating to the Privacy Program must be published in the Federal Register:

(1) DoD Component Privacy Program rules;

(2) Component exemption rules; and

(3) System notices.

b. See DoD 5025.1-M (reference (o)) and DoD Directive 5400.9 (reference (p)) for information pertaining to the preparation of documents for publication in the Federal Register.

2. The effect of publication in the Federal Register. Publication of a document in the Federal Register constitutes official public notice of the existence and content of the document.

3. DoD Component rules

a. Component Privacy Program procedures and Component exemption rules are subject to the rulemaking procedures prescribed in reference (p).

b. System notices are not subject to formal rulemaking and are published in the Federal Register as "Notices," not rules.

c. Privacy procedural and exemption rules are incorporated automatically into the Code of Federal Regulations (CFR). System notices are not published in the CFR.

4. Submission of rules for publication

a. Submit to the Defense Privacy Office, ODASD(A), all proposed rules implementing this Regulation in proper format (see references (o) and (p)) for publication in the Federal Register.

b. This Regulation has been published as a final rule in the Federal Register. Therefore, incorporate it into your Component rules by reference rather than by republication (see reference (p)).

c. DoD Component rules that simply implement this Regulation need only be published as final rules in the Federal Register (see references (o) and (p)).

d. Amendments to Component rules are submitted like the basic rules.

e. The Defense Privacy Office submits the rules and amendments thereto to the Federal Register for publication.

5. Submission of exemption rules for publication

a. No system of records within the Department of Defense shall be considered exempt from any provision of this Regulation until the exemption and the exemption rule for the system has been published as a final rule in the Federal Register (see subsection A.3. of this Chapter).

b. Submit exemption rules in proper format to the Defense Privacy Office. After review, the Defense Privacy Office will submit the rules to the Federal Register for publication.

c. Exemption rules require publication both as proposed rules and final rules (see DoD Directive 5400.9, reference (p)).

d. Section B. of this Chapter discusses the content of an exemption rule.

e. Submit amendments to exemption rules in the same manner used for establishing these rules.

6. Submission of system notices for publication

a. While system notices are not subject to formal rulemaking procedures, advance public notice must be given before a Component may begin to collect personal information or use a new system of records. The notice procedures require that:

(1) The system notice describes the contents of the record system and the routine uses for which the information in the system may be released.

(2) The public be given 30 days to comment on any proposed routine uses before implementation; and

(3) The notice contain the date on which the system will become effective.

c. Submit system notices to the Defense Privacy Office in the Federal Register format (see reference (p) and Appendix E). The Defense Privacy Office transmits the notices to the Federal Register for publication.

d. Section C. of this Chapter discusses the specific elements required in a system notice.

B. EXEMPTION RULES

1. General procedures. Subsection 2.a. of Chapter 5 provides the general guidance for establishing exemptions for systems of records.

2. Contents of exemption rules

a. Each exemption rule submitted for publication must contain the following:

(1) The record system identification and title of the system for which the exemption is claimed (see subsections C.2. and C.3. of this Chapter);

(2) The specific subsection of the Privacy Act under which exemptions for the system are claimed (for example, 5 U.S.C. 552a(j)(2), 5 U.S.C. 552a(k)(3); or 5 U.S.C. 552a(k)(7);

(3) The specific provisions and subsections of the Privacy Act from which the system is to be exempted (for example, 5 U.S.C. 552a(c)(3), or 5 U.S.C. 552a(d)(1)-(5)) (see Appendix D); and

(4) The specific reasons why an exemption is being claimed from each subsection of the Act identified.

b. Do not claim an exemption for classified material for individual systems of records, since the blanket exemption applies (see subsection A.3. of Chapter 5).

C. SYSTEM NOTICES

1. Contents of the system notices

a. The following data captions are included in each system notice:

(1) Systems identification (see subsection C.2. of this Chapter).

(2) System name (see subsection C.3. of this Chapter).

(3) System location (see subsection C.4. of this Chapter).

(4) Categories of individuals covered by the system (see subsection C.5. of this Chapter).

(5) Categories of records in the system (see subsection C.6. of this Chapter).

(6) Authority for maintenance of the system (see subsection C.7. of this Chapter).

(7) Purpose(s) (see subsection C.8. of this Chapter).

(8) Routine uses of records maintained in the system, including categories of users, uses, and purposes of such uses (see subsection C.8. of this Chapter).

(9) Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system (see subsection C.9. of this Chapter).

(10) Systems manager(s) and address (see subsection C.10. of this Chapter).

(11) Notification procedure (see subsection C.11. of this Chapter).

(12) Record access procedures (see subsection C.12. of this Chapter).

(13) Contesting records procedures (see subsection C.13. of this Chapter).

(14) Record source categories (see subsection C.14. of this Chapter).

(15) Systems exempted from certain provision of the Act (see subsection C.15. of this Chapter).

b. The captions listed in paragraph C.1.a. of this Chapter have been mandated by the Office of Federal Register and must be used exactly as presented.

c. A sample system notice is shown in Appendix E.

2. System identification. The system identifier must appear on all system notices and is limited to 21 positions, including Component code, file number and symbols, punctuation, and spacing.

3. System name

a. The name of the system reasonably identifies the general purpose of the system and, if possible, the general categories of individuals involved.

b. Use acronyms only parenthetically following the title or any portion thereof, such as, "Joint Uniform Military Pay System (JUMPS)." Do not use acronyms that are not commonly known unless they are preceded by an explanation.

c. The system name may not exceed 55 character positions including punctuation and spacing.

4. System location

a. For systems maintained in a single location provide the exact office name, organizational identity, and address or routing symbol.

b. For geographically or organizationally decentralized systems, specify each level of organization or element that maintains a segment of the system.

c. For automated data systems with a central computer facility and input/output terminals at several geographically separated locations, list each location by category.

d. When multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are contained in an address directory published as an appendix to the Component system notices in the Federal Register. Information concerning format requirements for

preparation of an address directory may be obtained from the project officer, Air Force Data Services Center (AFDSC/GNM), Washington, DC 20330.

e. If no address directory is used or the addresses in the directory are incomplete, the address of each location where a segment of the record system is maintained must appear under the "System Location" caption.

f. Classified addresses are not listed, but the fact that they are classified is indicated.

g. Use the standard U.S. Postal Service two letter state abbreviation symbols and zip codes for all domestic addresses.

5. Categories of individuals covered by the system

a. Set forth the specific categories of individuals to whom records in the system pertain in clear, easily understood, nontechnical terms.

b. Avoid the use of broad over-general descriptions, such as "all Army personnel" or "all military personnel" unless this actually reflects the category of individuals involved.

6. Categories of records in the system

a. Describe in clear, nontechnical terms the types of records maintained in the system.

b. Only documents actually retained in the system of records shall be described, not source documents that are used only to collect data and then destroyed.

7. Authority for maintenance of the system

a. Cite the specific provision of the federal statute or Executive Order that authorizes the maintenance of the system.

b. Include with citations for statutes the popular names, when appropriate (for example, Title 51, United States Code, Section 2103, "Tea-Tasters Licensing Act"), and for Executive Orders, the official title (for example, Executive Order No. 9397, "Numbering System for Federal Accounts Relating to Individual Persons").

c. Cite the statute or Executive Order establishing the Component for administrative housekeeping records.

d. If the Component is chartered by a DoD Directive, cite that Directive as well as the Secretary of Defense authority to issue the Directive. For example, "Pursuant to the authority contained in the National Security Act of 1947, as amended (10 U.S.C. 133d), the Secretary of Defense has issued DoD Directive 5105.21, the charter of the Defense Intelligence Agency (DIA) as a separate Agency of the Department of Defense under his control. Therein, the Director, DIA, is charged with the responsibility of maintaining all necessary and appropriate records."

8. Purpose or Purposes

a. List the specific purposes for maintaining the system of records by the Component.

b. Include the uses made of the information within the Component and the Department of Defense (so-called "internal routine uses").

9. Routine uses

a. The blanket routine uses (Appendix C) that appear at the beginning of each Component compilation apply to all systems notices unless the individual system notice specifically states that one or more of them do not apply to the system. List the blanket routine uses at the beginning of the Component listing of system notices (see paragraph B.6.d. of Chapter 4).

b. For all other routine uses, when practical, list the specific activity to which the record may be released, to include any routine automated system interface (for example, "to the Department of Justice, Civil Rights Compliance Division," "to the Veterans Administration, Office of Disability Benefits," or "to state and local health agencies").

c. For each routine user identified, include a statement as to the purpose or purposes for which the record is to be released to that activity (see subsection B.5. of Chapter 4).

d. Do not use general statements, such as, "to other federal agencies as required" or "to any other appropriate federal agency."

10. Policies and practices for storing, retiring, accessing, retaining, and disposing of records.

This caption is subdivided into four parts:

a. Storage. Indicate the medium in which the records are maintained. (For example, a system may be "automated, maintained on magnetic tapes or disks," "manual, maintained in paper files," or "hybrid, maintained in a combination of paper and automated form.") Storage does not refer to the container or facility in which the records are kept.

b. Retrievability. Specify how the records are retrieved (for example, name and SSN, name, SSN) and indicate whether a manual or computerized index is required to retrieve individual records.

c. Safeguards. List the categories of Component personnel having immediate access and those responsible for safeguarding the records from unauthorized access. Generally identify the system safeguards (such as storage in safes, vaults, locked cabinets or rooms, use of guards, visitor registers, personnel screening, or computer "fail-safe" systems software). Do not describe safeguards in such detail as to compromise system security.

d. Retention and Disposal. Indicate how long the record is retained. When appropriate, also state the length of time the records are maintained by the Component, when they are transferred to a Federal Records Center, length

of retention at the Records Center and when they are transferred to the National Archivist or are destroyed. A reference to a Component regulation without further detailed information is insufficient.

11. System manager or managers and address

a. List the title and address of the official responsible for the management of the system.

b. If the title of the specific official is unknown, such as for a local system, specify the local commander or office head as the systems manager.

c. For geographically separated or organizationally decentralized activities for which individuals may deal directly with officials at each location in exercising their rights, list the position or duty title of each category of officials responsible for the system or a segment thereof.

d. Do not include business or duty addresses if they are listed in the Component address directory.

12. Notification procedures

a. If the record system has been exempted from subsection (e)(4)(G) of the Privacy Act (reference (b)) (see subsection A.4. of Chapter 5), so indicate.

b. For all nonexempt systems, describe how an individual may determine if there are records pertaining to him or her in the system. The procedural rules may be cited, but include a brief procedural description of the needed data. Provide sufficient information in the notice to allow an individual to exercise his or her rights without referral to the formal rules.

c. As a minimum, the caption shall include:

(1) The official title (normally the system manager) and official address to which the request is to be directed;

(2) The specific information required to determine if there is a record of the individual in the system.

(3) Identification of the offices through which the individual may obtain access; and

(4) A description of any proof of identity required (see subsection A.3. of Chapter 3).

d. When appropriate, the individual may be referred to a Component official who shall provide this data to him or her.

13. Record access procedures

a. If the record system has been exempted from subsection (e)(4)(H) of reference (b) (see subsection A.4. of Chapter 5), so indicate.

b. For all nonexempt records systems, describe the procedures under which individuals may obtain access to the records pertaining to them in the system.

c. When appropriate, the individual may be referred to the system manager or Component offical to obtain access procedures.

d. Do not repeat the addresses listed in the Component address directory but refer the individual to that directory.

14. Contesting record procedures

a. If the record system has been exempted from subsection (e)(4)(H) of the Privacy Act (reference (b)) (see subsection A.4. of Chapter 5), so indicate.

b. For all nonexempt systems of records, state briefly how an individual may contest the content of a record pertaining to him or her in the system.

c. The detailed procedures for contesting record accuracy, refusal of access or amendment, or initial review and appeal need not be included if they are readily available elsewhere and can be referred to by the public. (For example, "The Defense Mapping Agency rules for contesting contents and for appealing initial determinations are contained in DMA Instruction 5400.11 (32 CFR Part 295c.")

d. The individual may also be referred to the system manager to determine these procedures.

15. Record source categories

a. If the record system has been exempted from subsection (e)(4)(I) of reference (b) (see subsection A.4. of Chapter 5), so indicate.

b. For all nonexempt systems of records, list the sources of the information in the system.

c. Specific individuals or institutions need not be identified by name, particularly if these sources have been granted confidentiality (see subsection C.2. of Chapter 5).

16. System exempted from certain provisions of the Act

a. If no exemption has been claimed for the system, indicate "None."

b. If there is an exemption claimed indicate specifically under which subsection of reference (b) it is claimed.

c. Cite the regulation and CFR section containing the exemption rule for the system. (For example, "Parts of this record system may be exempt under Title 5, United States Code, Sections 552a(k)(2) and (5), as applicable. See exemption rules contained in Army Regulation 340-21 (32 CFR Part 505).")

17. Maintaining the master DoD system notice registry

a. The Defense Privacy Office maintains a master registry of all DoD record systems notices.

b. Coordinate with the Defense Privacy Office to ensure that all new systems are added to the master registry and all amendments and alterations are incorporated into the master registry.

D. NEW AND ALTERED RECORD SYSTEMS

1. Criteria for a new record system

a. A new system of records is one for which there has been no system notice published in the Federal Register.

b. If a notice for a system of records has been canceled or deleted before reinstating or reusing the system, a new system notice must be published in the Federal Register.

2. Criteria for an altered record system. A system is considered altered whenever one of the following actions occurs or is proposed:

a. A significant increase or change in the number or type of individuals about whom records are maintained.

(1) Only changes that alter significantly the character and purpose of the record system are considered alterations.

(2) Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character and purpose of the system;

(3) Increases that change significantly the scope of population covered (for example, expansion of a system of records covering a single command's enlisted personnel to include all of the Component's enlisted personnel would be considered an alteration).

(4) A reduction in the number of individuals covered is not an alteration, but only an amendment (see subsection E.1. of this Chapter).

(5) All changes that add new categories of individuals to system coverage require a change to the "Categories of individuals covered by the system" caption of the notice (subsection C.5. of this Chapter) and may require changes to the "Purpose(s)" caption (subsection C.8. of this Chapter).

b. An expansion in the types or categories of information maintained.

(1) The addition of any new category of records not described under the "Categories of Records in System" caption is considered an alteration.

(2) Adding a new data element which is clearly within the scope of the categories of records described in the existing notice is an amendment (see subsection E.1. of this Chapter).

(3) All changes under this criterion require a change to the "Categories of Records in System" caption of the notice (see subsection C.6. of this Chapter).

c. An alteration in the manner in which the records are organized or the manner in which the records are indexed and retrieved.

(1) The change must alter the nature of use or scope of the records involved (for example, combining records systems in a reorganization).

(2) Any change under this criteria requires a change in the "Retrievability" caption of the system notice (see paragraph C.10.b. of this Chapter).

(3) If the records are no longer retrieved by name or personal identifier cancel the system notice (see subsection A.1. of Chapter 1).

d. A change in the purpose for which the information in the system is used.

(1) The new purpose must not be compatible with the existing purposes for which the system is maintained or a use that would not reasonably be expected to be an alteration.

(2) If the use is compatible and reasonably expected, there is no change in purpose and no alteration occurs.

(3) Any change under this criterion requires a change in the "Purpose(s)" caption (see subsection C.8. of this Chapter) and may require a change in the "Authority for maintenance of the system" caption (see subsection C.7. of this Chapter);

e. Changes that alter the computer environment (such as changes to equipment configuration, software, or procedures) so as to create the potential for greater or easier access.

(1) Increasing the number of offices with direct access is an alteration.

(2) Software releases, such as operating systems and system utilities that provide for easier access are considered alterations.

(3) The addition of an on-line capability to a previously batch-oriented system is an alteration.

(4) The addition of peripheral devices such as tape devices, disk devices, card readers, printers, and similar devices to an existing ADP system constitute an amendment if system security is preserved (see subsection E.1. of this Chapter).

(5) Changes to existing equipment configuration with on-line capability need not be considered alterations to the system if:

(a) The change does not alter the present security posture, or

(b) The addition of terminals does not extend the capacity of the current operating system and existing security is preserved;

(6) The connecting of two or more formerly independent automated systems or networks together creating a potential for greater access is an alteration.

(7) Any change under this caption requires a change to the "Storage" caption element of the systems notice (see paragraph C.10.a. of this Chapter).

3. Reports of new and altered systems

a. Submit a report of a new or altered system to the Defense Privacy Office before collecting information for or using a new system or altering an existing system (see Appendix F and subsection D.4. of this Chapter).

b. The Defense Privacy Office coordinates all reports of new and altered systems with the Office of the Assistant Secretary of Defense (Legislative Affairs) and the Office of the General Counsel, Department of Defense.

c. The Defense Privacy Office prepares for the DASD(A)'s approval and signature the transmittal letters sent to OMB and Congress (see subsection D.5. of this Chapter).

4. Time restrictions on the operation of a new or altered system

a. All time periods begin from the date the DASD(A) signs the transmittal letters (see paragraph D.3.c. of this Chapter). The specific time limits are:

(1) 60 days must elapse before data collection forms or formal instructions pertaining to the system may be issued.

(2) 60 days must elapse before the system may become operational (that is, collecting, maintaining, using, or disseminating records from the system) (see also subsection A.6. of this Chapter).

(3) 60 days must elapse before any public issuance of a Request for Proposal or Invitation to Bid for a new ADP or telecommunication system. (NOTE: Requests for delegation of procurement authority may be submitted to the General Services Administration during the 60 days' waiting period, but these shall include language that the Privacy Act reporting criteria have been reviewed and that a system report is required for such procurement.)

(4) Normally 30 days must elapse before publication in the Federal Register of the notice of a new or altered system (see subsection A.6. of this Chapter) and the preamble to the Federal Register notice must reflect the date the transmittal letters to OMB and Congress were signed by DASD(A).

b. Do not operate a system of records until the waiting periods have expired (see section D. of Chapter 10).

5. Outside review of new and altered systems reports. If no objections are received within 30 days of a submission to the President of the Senate, Speaker of the House of Representatives, and the Director, OMB, of a new or altered system report it is presumed that the new or altered systems have been approved as submitted.

6. Exemptions for new systems

See subsection A.5. of this Chapter for the procedures to follow in submitting exemption rules for a new system of records.

7. Waiver of time restrictions

a. The OMB may authorize a federal agency to begin operation of a system of records before the expiration of time limits set forth in subsection D.4. of this Chapter.

b. When seeking such a waiver, include in the letter of transmittal to the Defense Privacy Office an explanation why a delay of 60 days in establishing the system of records would not be in the public interest. The transmittal must include:

(1) How the public interest will be affected adversely if the established time limits are followed; and

(2) Why earlier notice was not provided.

c. When appropriate, the Defense Privacy Office shall contact OMB and attempt to obtain the waiver.

(1) If a waiver is granted, the Defense Privacy Office shall notify the subcommittee and submit the new or altered system notice along with any applicable procedural or exemption rules for publication in the Federal Register.

(2) If the waiver is disapproved, the Defense Privacy Office shall process the system the same as any other new or altered system and notify the subcommittee of the OMB decision.

d. Under no circumstances shall the routine uses for new or altered system be implemented before 30 days have elapsed after publication of the system notice containing the routine uses in the Federal Register. This period cannot be waived.

E. AMENDMENT AND DELETION OF SYSTEMS NOTICES

1. Criteria for an amended system notice

a. Certain minor changes to published systems notices are considered amendments and not alterations (see subsection D.2. of this Chapter).

b. Amendments do not require a report of an altered system (see subsection D.3. of this Chapter), but must be published in the Federal Register.

2. System notices for amended systems. When submitting an amendment for a system notice for publication in the Federal Register include:

a. The system identification and name (see subsections C.2. and C.3. of this Chapter).

b. A description of the nature and specific changes proposed.

c. The full text of the system notice is not required if the master registry contains a current system notice for the system (see subsection C.1. of this Chapter).

3. Deletion of system notices

a. Whenever a system is discontinued, combined into another system, or determined no longer to be subject to this Regulation, a deletion notice is required.

b. The notice of deletion shall include:

(1) The system identification and name.

(2) The reason for the deletion.

c. When the system is eliminated through combination or merger, identify the successor system or systems in the deletion notice.

4. Submission of amendments and deletions for publication

a. Submit amendments and deletions to the Defense Privacy Office for transmittal to the Federal Register for publication.

b. Include in the submission at least one original (not a reproduced copy) in proper Federal Register format (see Appendix G).

c. Multiple deletions and amendments may be combined into a single submission.

CHAPTER 7

TRAINING REQUIREMENTS

A. STATUTORY TRAINING REQUIREMENTS

The Privacy Act (reference (b)) requires each agency to establish rules of conduct for all persons involved in the design, development, operation, and maintenance of any system of record and to train these persons with respect to these rules.

B. OMB TRAINING GUIDELINES

The OMB guidelines require all agencies additionally to:

1. Instruct their personnel in their rules of conduct and other rules and procedures adopted in implementing the Act, and inform their personnel of the penalties for noncompliance.

2. Incorporate training on the special requirements of the Act into both formal and informal (on-the-job) training programs.

C. DoD TRAINING PROGRAMS

1. To meet these training requirements, establish three general levels of training for those persons who are involved in any way with the design, development, operation, or maintenance of any system of records. These are:

a. Orientation. Training that provides basic understanding of this Regulation as it applies to the individual's job performance. This training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

b. Specialized training. Training that provides information as to the application of specific provisions of this Regulation to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, and other specialists (reports, forms, records, and related functions), computer systems development personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, and anyone responsible for implementing or carrying out functions under this Regulation.

c. Management. Training designed to identify for responsible managers (such as, senior system managers, denial authorities, decision-makers, and the managers of the functions described in section A. of this Chapter) considerations that they shall take into account when making management decisions regarding the Privacy Program.

2. Include Privacy Act training in courses of training when appropriate. Stress individual responsibilities and advise individuals of their rights and responsibilities under this Regulation.

D. TRAINING METHODOLOGY AND PROCEDURES

1. Each DoD Component is responsible for the development of training procedures and methodology.

2. The Defense Privacy Office will assist the Components in developing these training programs and may develop Privacy training programs for use by all DoD Components.

3. All training programs shall be coordinated with the Defense Privacy Office to avoid duplication and to ensure maximum effectiveness.

E. FUNDING FOR TRAINING

Each DoD Component shall fund its own Privacy training program.

CHAPTER 8

REPORTS

A. REQUIREMENT FOR REPORTS

The Defense Privacy Office shall establish requirements for DoD Privacy Reports and DoD Components may be required to provide data.

B. SUSPENSE FOR SUBMISSION OF REPORTS

The suspenses for submission of all reports shall be established by the Defense Privacy Office.

C. REPORTS CONTROL SYMBOL

Any report established by this Chapter in support of the Privacy Program shall be assigned Report Control Symbol DD-COMP(A)1379. Special one-time reporting requirements shall be licensed separately in accordance with DoD Directive 5000.19 (reference (q)) and DoD Directive 5000.11 (reference (r)).

CHAPTER 9

INSPECTIONS

A. PRIVACY ACT INSPECTIONS

During internal inspections, Component inspectors shall be alert for compliance with this Regulation and for managerial, administrative, and operational problems associated with the implementation of the Defense Privacy Program.

B. INSPECTION REPORTING

1. Document the findings of the inspectors in official reports that are furnished the responsible Component officials. These reports, when appropriate, shall reflect overall assets of the Component Privacy Program inspected, or portion thereof, identify deficiencies, irregularities, and significant problems. Also document remedial actions taken to correct problems identified.

2. Retain inspections reports and later follow-up reports in accordance with established records disposition standards. These reports shall be made available to the Privacy Program officials concerned upon request.

CHAPTER 10

PRIVACY ACT ENFORCEMENT ACTIONS

A. ADMINISTRATIVE REMEDIES

Any individual who feels he or she has a legitimate complaint or grievanc against the Department of Defense or any DoD employee concerning any right granted by this Regulation shall be permitted to seek relief through appropri administrative channels.

B. CIVIL ACTIONS

An individual may file a civil suit against a DoD Component or its employe if the individual feels certain provisions of the Act have been violated (see 5 U.S.C. 552a(g), reference (b)).

C. CIVIL REMEDIES

In addition to specific remedial actions, reference (b) provides for the payment of damages, court cost, and attorney fees in some cases.

D. CRIMINAL PENALTIES

1. The act also provides for criminal penalties (see 5 U.S.C. 552a(i) (reference (b)). Any official or employee may be found guilty of a misdemeanc and fined not more than $5,000 if he or she willfully:

a. Discloses personal information to anyone not entitled to receive the information (see Chapter 4); or

b. Maintains a system of records without publishing the required public notice in the Federal Register (see Chapter 6).

2. A person who requests or obtains access to any record concerning anot individual under false pretenses may be found guilty of misdemeanor and fined up to $5,000.

E. LITIGATION STATUS SHEET

Whenever a complaint citing the Privacy Act is filed in a U.S. District C against the Department of Defense, a DoD Component, or any DoD employee, the responsible system manager shall notify promptly the Defense Privacy Office. The litigation status sheet at Appendix H provides a standard format for this notification. The initial litigation status sheet forwarded shall, as a mini provide the information required by items 1 through 6. A revised litigation status sheet shall be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment and opinion shal be provided to the Defense Privacy Office with the litigation status sheet reporting that judgment or opinion.

CHAPTER 11

MATCHING PROGRAM PROCEDURES

A. OMB MATCHING GUIDELINES

The OMB has issued special guidelines to be followed in programs that match the personal records in the computerized data bases of two or more federal agencies by computer (see Appendix I). These guidelines are intended to strike a balance between the interest of the government in maintaining the integrity of federal programs and the need to protect individual privacy expectations. They do not authorize matching programs as such and each matching program must be justified individually in accordance with the OMB guidelines.

B. REQUESTING MATCHING PROGRAMS

1. Forward all requests for matching programs to include necessary routine use amendments (see subsection C.9 of Chapter 6) and analysis and proposed matching program reports (see subsection E.6. of Appendix I) to the Defense Privacy Office.

2. The Defense Privacy Office shall review each request and supporting material and forward the report and system notice amendments to the Federal Register, OMB, and Congress, as appropriate.

3. Changes to existing matching programs shall be processed in the same manner as a new matching program report.

C. TIME LIMITS FOR SUBMITTING MATCHING REPORTS

1. No time limits are set by the OMB guidelines. However, in order to establish a new routine use for a matching program, the amended system notice must have been published in the Federal Register at least 30 days before implementation (see subsection A.6. of Chapter 6).

2. Submit the documentation required by subsection B.1.. of this Chapter to the Defense Privacy Office at least 45 days before the proposed initiation date of the matching program.

3. The Defense Privacy Office may grant waivers to the 45 days' deadline for good cause shown. Requests for waivers shall be in writing and fully justified.

D. MATCHING PROGRAMS AMONG DoD COMPONENTS

1. For the purpose of the OMB guidelines, the Department of Defense and all DoD Components are considered a single agency.

2. Before initiating a matching program using only the records of two or more DoD Components, notify the Defense Privacy Office that the match is to occur. The Defense Privacy Office may request further information from the Component proposing the match.

3. There is no need to notify the Defense Privacy Office of computer matches using only the records of a single Component.

E. ANNUAL REVIEW OF SYSTEMS OF RECORDS

The system manager shall review annually each system of records to determine if records from the system are being used in matching programs and whether the OMB Guidelines have been complied with.

Appendix A

SPECIAL CONSIDERATIONS FOR SAFEGUARDING PERSONAL INFORMATION IN ADP SYSTEMS

(See subsection D.2. of Chapter 1)

A. GENERAL

1. The Automated Data Processing (ADP) environment subjects personal information to special hazards as to unauthorized compromise alteration, dissemination, and use. Therefore, special considerations must be given to safeguarding personal information in ADP systems.

2. Personal information must also be protected while it is being processed or accessed in computer environments outside the data processing installation (such as, remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities).

3. ADP facilities authorized to process classified material have adequate procedures and security for the purposes of this Regulation. However, all unclassified information subject to this Regulation must be processed following the procedures used to process and access information designated "For Official Use Only" (see DoD 5400.7-R, reference (f)).

B. RISK MANAGEMENT AND SAFEGUARDING STANDARDS

1. Establish administrative, technical, and physical safeguards that are adequate to protect the information against unauthorized disclosure, access, or misuse (see Transmittal Memorandum No. 1 to OMB Circular A-71, reference (s)).

2. Technical and physical safeguards alone will not protect against unintentional compromise due to errors, omissions, or poor procedures. Proper administrative controls generally provide cheaper and surer safeguards.

3. Tailor safeguards to the type of system, the nature of the information involved, and the specific threat to be countered.

C. MINIMUM ADMINISTRATIVE SAFEGUARD

The minimum safeguarding standards as set forth in subsection D.2. of Chapter 1 apply to all personal data within any ADP system. In addition:

1. Consider the following when establishing ADP safeguards:

   a. The sensitivity of the data being processed, stored and accessed;

   b. The installation environment;

   c. The risk of exposure;

   d. The cost of the safeguard under consideration.

2. Label or designate output and storage media products (intermediate and final) containing personal information that do not contain classified material in such a manner as to alert those using or handling the information of the need for special protection. Designating products "For Official Use Only" in accordance with DoD 5400.7-R (reference (f)) satisfies this requirement.

3. Mark and protect all computer products containing classified data in accordance with DoD 5200.1-R (reference (a)) and DoD 5200.28-M (reference (t)).

4. Mark and protect all computer products containing "For Official Use Only" material in accordance with reference (f).

5. Ensure that safeguards for protected information stored at secondary sites are appropriate.

6. If there is a computer failure, restore all protected information being processed at the time of the failure using proper recovery procedures to ensure data integrity.

7. Train all ADP personnel involved in processing information subject to this Regulation in proper safeguarding procedures.

D. PHYSICAL SAFEGUARDS

1. For all unclassified facilities, areas, and devices that process information subject to this Regulation, establish physical safeguards that protect the information against reasonably identifiable threats that could result in unauthorized access or alteration.

2. Develop access procedures for unclassified computer rooms, tape libraries, micrographic facilities, decollating shops, product distribution areas, or other direct support areas that process or contain personal information subject to this Regulation that control adequately access to these areas.

3. Safeguard on-line devices directly coupled to ADP systems that contain or process information from systems of records to prevent unauthorized disclosure use or alteration.

4. Dispose of paper records following appropriate record destruction procedures.

E. TECHNICAL SAFEGUARDS

1. The use of encryption devices solely for the purpose of protecting unclassified personal information transmitted over communication circuits or during processing in computer systems is normally discouraged. However, when a comprehensive risk assessment indicates that encryption is cost-effective it may be used.

2. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.

3. Ensure that personal information is not inadvertently disclosed as residue when transferring magnetic media between activities.

4. When it is necessary to provide dial-up remote access for the processing of personal information, control access by computer-verified passwords. Change passwords periodically or whenever compromise is known or suspected.

5. Normally the passwords shall give access only to those data elements (fields) required and not grant access to the entire data base.

6. Do not rely totally on proprietary software products to protect personnel data during processing or storage.

F. SPECIAL PROCEDURES

1. System Managers shall:

a. Notify the ADP manager whenever personal information subject to this Regulation is to be processed by an ADP facility.

b. Prepare and submit for publication all system notices and amendments and alterations thereto (see subsection A.6. of Chapter 6).

c. Identify to the ADP manager those activities and individuals authorized access to the information and notify the manager of any changes to the access authorizations.

2. ADP personnel shall:

a. Permit only authorized individuals access to the information.

b. Adhere to the established information protection procedures and rules of conduct.

c. Notify the system manager and ADP manager whenever unauthorized personnel seek access to the information.

3. ADP installation managers shall:

a. Maintain an inventory of all computer program applications used to process information subject to this Regulation to include the identity of the systems of records involved.

b. Verify that requests for new programs or changes to existing programs have been published as required (see subsections D.1. and 2. of Chapter 6).

c. Notify the system manager whenever changes to computer installations, communications networks, or any other changes in the ADP environment occur that require an altered system report be submitted (see subsection D.2. of Chapter 6).

G. RECORD DISPOSAL

1. Dispose of records subject to this Regulation so as to prevent compromise (see subsection D.3. of Chapter 1). Magnetic tapes or other magnetic medium, may be cleared by degaussing, overwriting, or erasing. Unclassified carbon ribbons are considered destroyed when placed in a trash receptacle.

2. Do not use respliced waste computer products containing personal data.

H. RISK ASSESSMENT FOR ADP INSTALLATIONS THAT PROCESS PERSONAL DATA

1. A separate risk assessment is not required for ADP installations that process classified material. A simple certification by the appropriate ADP official that the facility is cleared to process a given level of classified material (such as, Top Secret, Secret, or Confidential) and that the procedures followed in processing "For Official Use Only" material are to be followed in processing personal data subject to this Regulation is sufficient to meet the risk assessment requirement.

2. Prepare a formal risk assessment for each ADP installation (to include those activities with terminals and devices having access to ADP facilities that processes personal information subject to this Regulation and that do not process classified material.

3. Address the following in the risk assessment: -

a. Identify the specific systems of records supported and determine their impact on the mission of the user.

b. Identify the threats (internal, external, and natural) to the data.

c. Determine the physical and operational (to include software) vulnerabilities.

d. Evaluate the relationships between vulnerabilities and threats.

e. Assess the impact of unauthorized disclosure or modification of the personal information.

f. Identify possible safeguards and their relationships to the threats to be countered.

g. Analyze the economic feasibility of adopting the identified safeguards.

h. Determine the safeguard to be used and develop implementation plans.

i. Discuss contingency plans including operational exercise plans.

j. Determine if procedures proposed are consistent with those identified in the system notices for system of records concerned.

k. Include a vulnerability assessment.

3. The risk assessment shall be reviewed by the appropriate Component officials.

4. Conduct a risk assessment at ~~least~~ every 5 years or when there is a change to the installation, its hardware, software, or administrative procedures that increase or decrease the likelihood of compromise or present new threats to the information.

5. Protect the risk assessment as it is a sensitive document.

6. Retain a copy of the risk assessment at the installation and make it available to appropriate inspectors and authorized personnel.

7. Include a summary of the current risk assessment with any report of new or altered system submitted in accordance with subsection D.3. of Chapter 6 for any system from which information will be processed.

8. Complete a formal risk assessment at the beginning of the design phase for each new unclassified ADP installation and before beginning the processing of personal data on a regular basis in existing ADP facility that do not process classified data.

APPENDIX B

SPECIAL CONSIDERATIONS FOR SAFEGUARDING PERSONAL INFORMATION DURING WORD PROCESSING

(See subsection D.2. of Chapter 1)

A. INTRODUCTION

1. Normally, word processing support is provided under two general concepts. They are:

a. Word processing centers (WPCs) and

b. Work groups or clusters.

2. A WPC generally provides support to one or more functional areas. Characteristically, the customer delivers (by written draft or dictation) the information to be processed to the WPC. The WPC processes the information and returns it to the customer. There are generally two types of WPCs.

a. A WPC may operate independent of the customer's function, providing service in much the same manner as a data processing installation provides ADP support, or a message center provides electronic message service, or

b. A WPC may work within a customer's function providing support to that function. The support being centralized in a WPC to take advantage of increased productivity.

3. A work group or cluster generally consists of one or more pieces of word processing equipment that are integrated into the functional office support system. The overall word processing and functional management may be one and the same. Depending on the size of the support job, there may be a work group or cluster manager. Normally, however, they will be located within or in close proximity to the functional area supported. Information flows in and out of the work group or cluster by normal office routine and the personnel are an integral part of the office staff.

B. MINIMUM STANDARDS OF PROTECTION

1. Regardless of configuration (WPC or work group), all personal data processed using word processing equipment shall be afforded the standards of protection required by subsection D.2. of Chapter 1.

2. The remaining special considerations discussed in this Appendix are primarily for WPCs operating independent of the customer's function. However, managers of other WPCs, work groups, and work clusters are encouraged to consider and adopt, when appropriate, the special considerations discussed herein.

3. WPCs that are not independent of a customer's function, work groups, and work clusters are not required to prepare formal written risk assessments (see section H., below).

C. WPC INFORMATION FLOW

1. In analyzing procedures required to safeguard adequately personal information in a WPC, the basic elements of WPC information flow and control must be considered. These are:

a. Information receipt.

b. Information processing.

c. Information return.

d. Information storage or filing.

2. WPCs do not control information acquisition or its ultimate use by the customers and, therefore, these are not addressed.

D. SAFEGUARDING INFORMATION DURING RECEIPT

1. The word processing manager shall establish procedures

a. That require each customer who requests that information subject to this Regulation be processed to identify specifically that information to the WPC personnel. This may be done by:

(1) Providing a check-off type entry on the WPC work requests;

(2) Requiring that the WPC work requests be stamped with a special legend, or that a special notation be made on the work requests;

(3) Predesignating specifically a class of documents as coming within the provisions of this Regulation (such as, all officer effectiveness reports, all recall rosters, and all medical protocols).

(4) Using a special cover sheet both to alert the WPC personnel as to the type information, and to protect the document during transmittal;

(5) Requiring an oral warning on all dictation; or

(6) Any other procedures that ensure the WPC personnel are alerted to the fact that personal data subject to this Regulation is to be processed.

b. To ensure that the operators or other WPC personnel receiving data for processing that has not been identified to be under the provisions of this Regulation but that appear to be personal promptly call the information to the attention of the WPC supervisor or the customer;

c. To ensure that any request for the processing of personal data that the customer has not identified as being in a system of records and that appears to meet the criteria set forth in subsection A.1. of Chapter 1 is called to the attention of the appropriate supervisory personnel and system manager.

2. The WPC supervisor shall ensure that personal information is not inadvertently compromised within the WPC.

E. SAFEGUARDING INFORMATION DURING PROCESSING

1. Each WPC supervisor shall establish internal safeguards that shall protect personal data from compromise while it is being processed.

2. Physical safeguards may include:

a. Controls on individual access to the center;

b. Machine configurations that reduce external access to the information being processed, or arrangements that alert the operator to the presence of others;

c. Using certain specific machines to process personal data;

d. Any other physical safeguards, to include special technical arrangements that will protect the data during processing.

3. Other safeguards may include:

a. Using only certain selected operators to process personal data;

b. Processing personal data only at certain times during the day without the WPC manager's specific authorization;

c. Using only certain tapes or diskettes to process and store personal data;

d. Using continuous tapes for dictation of personal data;

e. Requiring all WPC copies of documents to be marked specifically so as to prevent inadvertent compromise;

f. Returning extra copies and mistakes to the customer with the product;

g. Disposing of waste containing personal data in a special manner;

h. Any other local procedures that provide adequate protection to the data being processed.

F. SAFEGUARDING INFORMATION DURING RETURN

1. The WPC shall protect the data until it is returned to the customer or placed into a formal distribution channel.

2. In conjunction with the appropriate administrative support personnel and the WPC customers, the WPC manager shall establish procedures that protect the information from the time word processing is completed until it is returned to the customer.

3. Safeguarding procedures may include:

a. Releasing products only to specifically identified individuals;

b. Using sealed envelopes to transmit products to the customer;

c. Using special cover sheets to protect products similar to the one discussed in subparagraph D.1.a.(4), above;

d. Handcarrying products to the customers;

e. Using special messengers to return the products;

f. Any other procedures that protect adequately products from compromise while they are awaiting return or being returned to the customer.

G. SAFEGUARDS DURING STORAGE

1. The WPC manager shall ensure that all personal ~~data~~ retained in the center for any purpose (including samples) are protected properly.

2. Safeguarding procedures may include:

a. Marking all hard copies retained with special legends or designators;

b. Storing media containing personal data in separate files or areas;

c. Marking the storage containers for media containing personal data with special legends or notations;

d. Restricting the reuse of media used to process personal data or erasing automatically the media before reuse;

e. Establishing special criteria for the WPC retention of media used to store and process personal data;

f. Returning the media to the customer for retention with the file copies of the finished products;

g. Discouraging, when practical, the long-term storage of personal data in any form within the WPC;

h. Any other filing or storage procedures that safeguard adequately any personal information retained or filed within the WPC.

H. RISK ASSESSMENT FOR WPCs

1. Each WPC manager shall ensure that a formal, written risk assessment is prepared for each WPC that processes personal information subject to this Regulation.

2. The assessment shall address the areas discussed in sections D., E., and G. of this Appendix, as well as any special risks that the WPC location, configuration, or organization may present to the compromise or alteration of personal data being processed or stored.

3. A risk assessment shall be conducted at least every 5 years or whenever there is a change of equipment, equipment configuration, WPC location, WPC configuration or modification of the WPC facilities that either increases or decreases the likelihood of compromise of personal data.

4. Copies of the risk assessment shall be retained by the WPC manager and made available to appropriate inspectors, as well as to personnel studying equipment for facility upgrading or modification.

5. Every new WPC shall have a formal risk assessment completed before beginning the processing of personal data.

I. SPECIAL CONSIDERATIONS IN WPC DESIGN AND MODIFICATION

Procedures shall be established to ensure that all personnel involved in the design of WPCs or the acquisition of word processing equipment are aware the special considerations required when processing personal data subject to Regulation.

APPENDIX C

DoD BLANKET ROUTINE USES

(Subsection B.5. of Chapter 4)

A. ROUTINE USE - LAW ENFORCEMENT

If a system of records maintained by a DoD Component to carry out its functi indicates a violation or potential violation of law, whether civil, criminal, o regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

B. ROUTINE USE - DISCLOSURE WHEN REQUESTING INFORMATION

A record from a system of records maintained by a Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

C. ROUTINE USE - DISCLOSURE OF REQUESTED INFORMATION

A record from a system of records maintained by a Component may be disclosed to a federal agency, in response to its request, in connection with the hiring, or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

D. ROUTINE USE - CONGRESSIONAL INQUIRIES

Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

E. ROUTINE USE - PRIVATE RELIEF LEGISLATION

Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the OMB in connection with the review of private relief legislation as set forth in OMB Circular A-19 (reference (u)) at any stage of the legislative coordination and clearance process as set forth in that Circular.

F. ROUTINE USE - DISCLOSURES REQUIRED BY INTERNATIONAL AGREEMENTS

A record from a system of records maintained by a Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

G. ROUTINE USE - DISCLOSURE TO STATE AND LOCAL TAXING AUTHORITIES

Any information normally contained in Internal Revenue Service (IRS) Form W-2 which is maintained in a record from a system of records maintained by a Component may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., Sections 5516, 5517, and 5520 (reference (v)) and only to those state and local taxing authorities for which an employee or military member is or was subject to tax regardless whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07 (reference (w)).

H. ROUTINE USE - DISCLOSURE TO THE OFFICE OF PERSONNEL MANAGEMENT

A record from a system of records subject to the Privacy Act and maintained by a Component may be disclosed to the Office of Personnel Management (OPM), concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

NOTE: Do not include the references to the Reference section (page ix) of this Regulation when preparing the blanket exemptions for inclusion in other publications.

APPENDIX D

PROVISIONS OF THE PRIVACY ACT FROM WHICH A GENERAL OR SPECIFIC EXEMPTION MAY BE CLAIMED

(See subsection A.4 of Chapter 5)

Exemption		Section of the Privacy Act	
(j)(2)	(k)(1-7)		
No	No	(b)(1)	Disclosures within the Department of Defense
No	No	(2)	Disclosures to the public.
No	No	(3)	Disclosures for a "Routine Use."
No	No	(4)	Disclosures to the Bureau of Census.
No	No	(5)	Disclosures for statistical research and reporting.
No	No	(6)	Disclosures to the National Archives.
No	No	(7)	Disclosures for law enforcement purposes.
No	No	(8)	Disclosures under emergency circumstances.
No	No	(9)	Disclosures to the Congress.
No	No	(10)	Disclosures to the General Accounting Office.
No	No	(11)	Disclosures pursuant to court orders.
No	No	(12)	Disclosure to consumer reporting agencies.
No	No	(c)(1)	Making disclosure accountings.
No	No	(2)	Retaining disclosure accountings.
Yes	Yes	(c)(3)	Making disclosure accounting available to the individual.
Yes	No	(c)(4)	Informing prior recipients of corrections.
Yes	Yes	(d)(1)	Individual access to records.
Yes	Yes	(2)	Amending records.
Yes	Yes	(3)	Review of the Component's refusal to amend a record.
Yes	Yes	(4)	Disclosure of disputed information.
Yes	Yes	(5)	Access to information compiled in anticipation of civil action.

Exemption (j)(2)	Exemption (k)(1-7)	Section of the Privacy Act	
Yes	Yes	(e)(1)	Restrictions on collecting information.
Yes	No	(e)(2)	Collecting directly from the individual.
Yes	No	(3)	Informing individuals from whom information is requested.
No	No	(e)(4)(A)	Describing the name and location of the system.
No	No	(B)	Describing categories of individuals.
No	No	(C)	Describing categories of records.
No	No	(D)	Describing routine uses.
No	No	(E)	Describing records management policies and practices
No	No	(F)	Identifying responsible officials.
Yes	Yes	(e)(4)(G)	Procedures for determining if a system contains a record on an individual.
Yes	Yes	(H)	Procedures for gaining access.
Yes	Yes	(I)	Describing categories of information sources.
Yes	No	(e)(5)	Standards of accuracy.
No	No	(e)(6)	Validating records before disclosure.
No	No	(e)(7)	Records of First Amendment activities.
No	No	(e)(8)	Notification of disclosure under compulsory legal process.
No	No	(e)(9)	Rules of conduct.
No	No	(e)(10)	Administrative, technical and physical safeguards.
No	No	(11)	Notice for new and revised routine uses.
Yes	Yes	(f)(1)	Rules for determining if an individual is subject of a record.

Exemption		Section of the Privacy Act	
(j)(2)	(k)(1-7)		
Yes	Yes	(f)(2)	Rules for handling access requests.
Yes	Yes	(f)(3)	Rules for granting access.
Yes	Yes	(f)(4)	Rules for amending records.
Yes	Yes	(f)(5)	Rules regarding fees.
Yes	No	(g)(1)	Basis for civil action.
Yes	No	(g)(2)	Basis for judicial review and remedies for refusal to amen
Yes	No	(g)(3)	Basis for judicial review and remedies for denial of acces
Yes	No	(g)(4)	Basis for judicial review and remedies for other failure comply.
Yes	No	(g)(5)	Jurisdiction and time limits.
Yes	No	(h)	Rights of legal guardians.
No	No	(i)(1)	Criminal penalties for unauthorized disclosure.
No	No	(2)	Criminal penalties for failure to publish.
No	No	(3)	Criminal penalties for obtaining records under false pretenses.
[1]Yes	No	(j)	Rulemaking requirement.
N/A	No	(j)(1)	General exemption for the Central Intelligence Agency
N/A	No	(j)(2)	General exemption for crimina law enforcement records.
Yes	N/A	(k)(1)	Exemption for classified material.
N/A	N/A	(k)(2)	Exemption for law enforcement material.
Yes	N/A	(k)(3)	Exemption for records pertaining to Presidential protection.
Yes	N/A	(k)(4)	Exemption for statistical re
Yes	N/A	(k)(5)	Exemption for investigatory material compiled for dete mining suitability for employment or service.
Yes	N/A	(k)(6)	Exemption for testing or exa ination material.

Exemption (j)(2)	Exemption (k)(1-7)	Section of the Privacy Act	
Yes	N/A	(k)(7)	Exemption for promotion evaluation materials used by the Armed Forces.
Yes	No	(1)(1)	Records stored in GSA records centers.
Yes	No	(1)(2)	Records archived before September 27, 1975.
Yes	No	(1)(3)	Records archived on or after September 27, 1975.
Yes	No	(m)	Applicability to government contractors.
Yes	No	(n)	Mailing lists.
[1]Yes	No	(o)	Reports on new systems.
[1]Yes	No	(p)	Annual report.

[1] See subsection A.4. of Chapter 5.

APPENDIX E

(See Chapter 4, DoD 5025.1-M (reference (o)) for additional format information[1])

SAMPLE OF NEW OR ALTERED SYSTEM OF RECORDS NOTICE IN FEDERAL REGISTER FORMAT

(See Subsection A.6. of Chapter 6)

DEPARTMENT OF DEFENSE

Defense Nuclear Agency

Privacy Act of 1974

New System of Records

AGENCY: Defense Nuclear Agency (DNA)

ACTION: Notice of a new record system

SUMMARY: The Defense Nuclear Agency is adding a new system of records to its inventory of systems of records subject to the Privacy Act of 1974. The system notice for the new system is set forth below.

DATES: This system shall be effective - unless comments are received which result in a contrary determination.

ADDRESS: Send comments to the System Manager identified in the system notice.

FOR FURTHER INFORMATION CONTACT:

Robert L. Brittigan,
General Counsel,
Defense Nuclear Agency,
Washington, D.C. 20305,
Telephone (202) 325-7681.

SUPPLEMENTARY INFORMATION: The Defense Nuclear Agency record system notice as prescribed by the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have appeared in the FEDERAL REGISTER on September 28, 1981 (46 FR 51073) and February 16, 1982 (47 FR 6829).

---

[1] Prepare Federal Register documents on 8½ by 11 inch plain bond paper. Margins shall be 1 inch all around and text shall be double-spaced.

The Defense Nuclear Agency has submitted a new system report on March 27, 1982, for this system of records under the provisions of 5 U.S.C. 552a(o) of the Privacy Act.

M. S. Healy
OSD Federal Register Liaison Officer
Department of Defense

SAMPLE

HDNA 609-03

System name:

Personnel Exposed to Radiation from Nuclear Tests.

System Location:

Headquarters, Defense Nuclear Agency, Washington, D.C. 20305, Main computer location.

Categories of individuals covered by the system:

All DoD and DoD-affiliated personnel, military and civilian, who participated in the U.S. Government atmospheric nuclear test programs in the Pacific and at the Nevada Test Site.

Categories of records in the system:

Personal information consisting of name, rank, service number, last known or current address, dates of test participation, exposure and unit of assignment.

Authority for maintenance of the system:

10 U.S.C. Section 133, Powers of an Executive Department of a Military Department to Prescribe Departmental Regulations; 10 U.S.C. Section 133, Secretary of Defense: Appointment, Powers, Duties and Delegation by; DoD Directive 5105.31, "Defense Nuclear Agency (DNA)."

Purpose(s): To identify those individuals who may have been exposed to radiation from nuclear atmospheric test conducted by the U.S. Government in the Pacific or at the Nevada Test Site.

Information is provided to the medical services of all the Military Departments to identify military and retired personnel who were exposed to ionizing radiator during testing.

Routine uses of records maintained in the system including categories of users, and the purpose of such uses:

To the National Research Council and Center for Disease Control to determine the effects of ionizing radiation for the limited purpose of conducting epidemiological studies of the atmospheric nuclear weapons tests on DoD participants in those tests.

To the Department of Energy (DoE) to identify DoE contractor personnel exposed to ionizing radiation during nuclear testing for the limited purpose of conducting epidemiological studies of radiation effects of individuals so identified.

To the Department of Transportation (DoT) for the limited purpose of identifying DoT and DoT-affiliated personnel exposed to ionizing radiation during nuclear testing.

To the Veterans Administration to make determinations on service-connected disability for the purpose or resolving claims.

Policies and Practices for storing, retrieving, accessing, retaining, and disposing of records in the system.

Storage: Paper records in file folders; computer magnetic tape disks and printouts in secure computer facility.

Retrievability: Paper records filed in folders and computer magnetic tape and disk retrieved by name.

Safeguards: Paper records are filed in folders stored in locked security safes. Magnetic tapes stored in a vault in a secure computer area.

Retention and disposal: Paper records are retained until information is transferred to magnetic tapes, then destroyed. Magnetic tapes and disks are retained indefinitely.

System manager(s) and address: Director, Defense Nuclear Agency, ATTN: Privacy Act Officer, Washington, D.C. 20305, telephone (202) 325-7681.

Notification procedure: Information may be obtained from the System Manager.

Record access procedures: Requests should be addressed to the System Manager.

Contesting record procedures: The agency's rules for contesting contents and appealing initial determinations are contained in DNA Instruction 5400.11 (32 CFR Part 291a). Additional information may be obtained from the System Manager.

Record source categories: DNA records, searches of DoD records by other DoD Components, and from individuals voluntarily contacting DNA by telephone or mail.

Systems exempted from certain provision of the Act: None.

APPENDIX F

FORMAT FOR NEW OR ALTERED SYSTEM REPORT

(See subsection D.3. of Chapter 6)

The report on a new or altered system shall consist of a transmittal letter, a narrative statement, and include supporting documentation.

A. TRANSMITTAL LETTER. The transmittal letter to the Director, Defense Privacy Office, ODASD(A), shall include any request for waivers as set forth in subsection D.7. of Chapter 6. The narrative statement shall be attached thereto.

B. NARRATIVE STATEMENT. The narrative statement is typed in double space on standard bond paper in the format shown at attachment 1. The statement includes

1. System identification and name. This caption sets forth the identification and name of the system (see subsections C.2. and C.3. of Chapter 6).

2. Responsible official. The name, title, address, and telephone number of the privacy official responsible for the report and to whom inquiries and comments about the report may be directed by Congress, the Office of Management and Budget, or Defense Privacy Office.

3. Purpose of the system or nature of the change proposed. Describe the purpose of the new system. For an altered system, describe the nature of the change being proposed.

4. Authority for the system. See subsection C.7. of Chapter 6.

5. Number of individuals. The approximate number of individuals about whom records are to be maintained.

6. Information on First Amendment activities. Describe any information to be kept on the exercise of individual's First Amendment rights and the basis for maintaining it as provided for in subsection A.5. of Chapter 1.

7. Measures to ensure information accuracy. If the system is to be used to make determinations about the rights, benefits, or entitlements of individuals; describe the measures being established to ensure the accuracy, currency, relevance, and completeness of the information used for these purposes.

8. Other measures to ensure system security: Describe the steps taken to minimize the risk of unauthorized access to the system. A more detailed assessment of security risks and specific administrative, technical, and physical safeguards shall be available for review upon request.

9. Relationship to state and local government activities Describe the relationship of the system to state or local government activities that are the sources, recipients, or users of the information in the system.

C. SUPPORTING DOCUMENTATION. Item 10 of the narrative is captioned Supporting Documents. A positive statement for this caption is essential for those enclosures that are not required to be enclosed. For example, "No changes to the existing Army procedural or exemption rules (32 CFR Part 505) are required for this proposed system." List in numerical sequence only those enclosures that are actually furnished. The following are typical enclosures that may be required:

1. For a new system, an advance copy of the system notice which is proposed for publication. For an altered system (see subsection E.4. of Chapter 6) an advance copy of the notice reflecting the specific changes proposed.

2. An advance copy of any new rules or changes to the published Component rules to be issued for the new or altered system. If no change to existing rules is required, so state in the narrative.

3. An advance copy of any proposed exemption rule if the new or altered system is to be exempted in accordance with Chapter 5. If there is no exemption, so state in the narrative.

4. Any other supporting documentation that may be pertinent or helpful in understanding the need for the system or clarifying its intended use. While not required, such documentation, when available, is helpful in evaluating the new or altered system.

Attachments - 2
1. Format for Narrative Statement
2. Sample Report

SAMPLE

DEPARTMENT OF DEFENSE

(Component Name)

REPORT ON NEW (OR ALTERED) SYSTEM UNDER

THE PRIVACY ACT OF 1974

(Indicate none or not applicable, as appropriate).

1. System Identification and name:

2. Responsible official:

3. Purpose(s) of the System: (for a new system only) or
Nature of the Change(s) Proposed: (for altered system)

4. Authority for the System:

5. Number of Individuals:

6. Information on First Amendment Activities:

7. Measures to Ensure Information Accuracy:

8. Other Measures to Ensure System Security:

9. Relations to State or Local Government Activities:

10. Supporting Documentation: (Indicate here, as a positive statement, those enclosures not required as set forth in section C. of the format instructions.)

SIGNATURE BLOCK OF SUBMITTING OFFICIAL

SAMPLE REPORT

DEPARTMENT OF DEFENSE

Defense Nuclear Agency

REPORT ON NEW SYSTEM UNDER THE PRIVACY ACT OF 1974

1. System Identification and Name: HDNA 609-03, entitled "Personnel Exposed To Radiation From Nuclear Tests."

2. Responsible Official: Robert L. Brittigan, General Counsel, Defense Nuclear Agency, Washington, D.C. 20305. Telephone: Area Code 202 325-7781.

3. Purpose of the System: To consolidate into one system the names, addresses, and exposures of all DoD or DoD-associated personnel who may have been exposed to ionizing radiation during the atmospheric nuclear testing programs in the Pacific and at the Nevada Test Site.

4. Authority for the System: See "Authority for Maintenance of the System" caption of the attached proposed system notice.

5. Number of Individuals: Approximately 300,000 individuals will be affected by this new system, since the system includes all DoD and DoD-affiliated participants in the atmospheric nuclear tests program.

6. Information on First Amendment Activities: None.

7. Measures to Ensure Information Accuracy: Records consist of personal data to be provided by the individual such as name, rank, service number, last known or current address, dates of test participation, exposure date, if available, and unit of assignment. When the information has been obtained from sources other than the individual, follow-up is attempted to ensure accuracy.

8. Other Measures to Ensure System Security:

a. Paper records before processing for computer storage are retained in locked filing cabinets located in limited access facilities at DNA Headquarters and the Armed Forces Radiobiology Research Institute.

b. Privacy data in the Headquarters, DNA, ADP facility is afforded the same protection as classified data in that the DNA computer system employs a File Security System (FSS) to protect classified and privacy data files from being accessed by unauthorized users.

9. Relations to State and Local Government Activities: None.

10. Supporting Documentation: No changes to existing procedural or exemption rules are required for this proposed new system.

Robert L. Brittigan
General Counsel

Enclosures - 2
1. Advance copy of proposed system notice.
2. Copy of tasking memorandum from the Assistant Secretary of Defense (Manpower, Reserve Affairs, and Logistics) to the Director, Defense Nuclear Agency, "DoD Personnel Participation in Atmospheric Nuclear Weapons Testing," January 28, 1978.

(NOTE: Enclosures are not included in the sample, above.)

APPENDIX G

(See Chapter 4, DoD 5025.1-M (reference (o)) for additional format information)

SAMPLE DELETIONS AND AMENDMENTS TO SYSTEMS NOTICES IN FEDERAL REGISTER FORMAT

(See subsection E.4. of Chapter 6)

DEPARTMENT OF DEFENSE

Department of Air Force

PRIVACY ACT OF 1974

Deletions and Amendments to Systems of Records Notices

AGENCY: Department of the Air Force

ACTION: Notice of deletions and amendments to systems of records.

SUMMARY: The Air Force proposes to delete three and amend two notices for systems of records subject to the Privacy Act of 1974. The specific changes to the notices being amended are set forth below followed by the system notices, as amended, published in their entirety.

DATES: These systems notices shall be amended as proposed without further notice on unless comments are received that would result in a contrary determination.

ADDRESS: Send comments to the system manager identified in the particular system notice concerned.

FOR FURTHER INFORMATION CONTACT:

Mr. Jon E. Updike
HQ USAF/DAAD(S)
The Pentagon, Washington, D.C. 20330
Telephone: (202) 694-3431

SUPPLEMENTARY INFORMATION: The Air Force systems of records notices inventory subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published to date in the Federal Register as follows:

FR Doc.	80-28255	(46 FR 50785)	September 28, 1980
FR Doc.	80-31218	(46 FR 56774)	October 28, 1980
FR Doc.	80-32284	(46 FR 58195)	November 8, 1980
FR Doc.	80-33780	(46 FR 59996)	November 23, 1980

The proposed amendments are not within the purview of the provisions of 5 U.S.C. 552a(o) which requires the submission of an altered system report.

M. S. Healy
OSD Federal Register Liaison Officer
Department of Defense

DELETIONS

F01001 OQPTFLA

System name: Human Reliability for Special Missions

Reason: This system is covered by F03004 AFDPMDB Advanced Personnel Data System (APDS) (46 FR 50821 (August 28, 1981)).

F01003 OBXQPCA

System name: Cadet Promotion List

Reason: This system has been incorporated into F03502 AFA A Cadet Management System (46 FR 50875 (July 28, 1981)).

F01102 OYUEBLA

System name: Locator or Personnel Data file

Reason: This system is covered by F01102 DAYX A Base, Unit, and Organizational Military and Civilian Personnel Locator Files (46 FR 50800 (October 28, 1981)).

AMENDMENTS

F03501 DPMDQIA

System name: Military Personnel Records System

Changes:

System Location: In line 8, change "Adjustment" to "Adjutant".

External users, uses and purposes:

Add at end:

"American National Red Cross. Information to Local Red Cross offices for emergency assistance to military members, dependents, relatives, or other persons if conditions are compelling."

"Drug Enforcement Administration" (added to those agencies listed under Department of Justice).

"Department of Labor: Bureau of Employees' Compensation - medical information for claims of civilian employees formerly in military service; Employment and Training Administration - verification of service-related information for unemployment compensation claims; Labor-Management Services Administration - for investigations of possible violations of labor laws and preemployment investigations; National Research Council - for medical research purposes; U.S. Soldiers' and Airmen's Home - service information to determine eligibility."

F03504 OJMPLSC

System name: Assessments Screening Records

Changes:

System location: In line 1, change "3700 Personnel Processing Group" to "3507 Airman Classification Squadron."

Retention and disposal: Delete entry and substitute: "Records on airmen accepted for sensitive or high risk assignments are retained in the office files for 18 months, then destroyed. Records of nonselectees are retained in office files for 1 year, then destroyed. Destruction is by tearing into pieces, shredding, pulping, macerating, or burning."

Systems manager: In line 1, change "3700 PPGP-(CCO)," to "3507 Airman Classification Squadron."

Record source categories: Add at end, "peers, character references, and the individual member."

APPENDIX H

LITIGATION STATUS SHEET

(See Section E. of Chapter 10)

1. Case Number[1]

2. Requester

3. Document Title or Description[2]

4. Litigation

   a. Date Complaint Filed
   b. Court
   c. Case File Number[1]

5. Defendants (DoD Component and individual)

6. Remarks (brief explanation of what the case is about)

7. Court Action

   a. Court's Finding
   b. Disciplinary Action (as appropriate)

8. Appeal (as appropriate)

   a. Date Complaint Filed
   b. Court
   c. Case File Number[1]
   d. Court's Finding
   e. Disciplinary Action (as appropriate)

[1] Number used by the Component for reference purposes
[2] Indicate the nature of the case, such as, "Denial of access," "Refusal to amend," "Incorrect records," or other violations of the Act (specify).

NOTE: This is the same format used in Appendix C, DoD 5400.7-R (reference (f)). To standardize for field elements, we have not changed the format.

APPENDIX I

OFFICE OF MANAGEMENT AND BUDGET

Matching Guidelines

(See subsection A.1. of Chapter 11)

A. PURPOSE. These guidelines supplement and shall be used in conjunction with OMB Guidelines on the Administration of the Privacy Act of 1974, issued in July 1, 1975, and supplemented on November 21, 1975. They replace earlier guidance on conducting computerized matching programs issued on March 30, 1979. They are intended to help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching. They are designed to address the concerns expressed by the Congress in the Privacy Act of 1974 that "the increasing use of computers and sophisticated information technology, while essential to the efficient operation of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information." These guidelines do not authorize activities that are not permitted by law, nor do they prohibit activities expressly required to be performed by law. Complying with these guidelines, however, does not relieve a federal agency of the obligation to comply with the provisions of the Privacy Act, including any provisions not cited in these guidelines.

B. SCOPE. These guidelines apply to all agencies subject to the Privacy Act of 1974 (5 U.S.C. 552a) and to all matching programs:

1. Performed by a federal agency, whether the personal records used in the match are federal or nonfederal.

2. For which a federal agency discloses any personal records for use in a matching program performed by any other federal agency or any nonfederal organization.

C. EFFECTIVE DATE. These guidelines are effective on May 11, 1982.

D. DEFINITIONS. For the purposes of the Guidelines, all the terms defined in the Privacy Act of 1974 apply.

1. Personal Record. Any information pertaining to an individual that is stored in an automated system of records; for example, a data base which contains information about individuals that is retrieved by name or some other personal identifier.

2. Matching Program. A procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of nonfederal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among a number of participants. Matching programs do not include the following:

a. Matches that do not compare a substantial number of records, such as, comparison of the Department of Education's defaulted student loan data base with the Office of Personnel Management's federal employee data base would be covered; comparison of six individual student loan defaultees with the OPM file would not be covered.

b. Checks on specific individuals to verify data in an application for benefits done reasonably soon after the application is received.

c. Checks on specific individuals based on information which raises questions about an individual's eligibility for benefits or payments done reasonably soon after the information is received.

d. Matches done to produce aggregate statistical data without any personal identifiers.

e. Matches done to support any research or statistical project when the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.

f. Matches done by an agency using its own records.

3. Matching Agency. The federal agency which actually performs the match.

4. Source Agency. The federal agency which discloses records from a system of records to be used in the match. Note that in some circumstances a source agency may be the instigator and ultimate beneficiary of the matching program, as when an agency lacking computer resources uses another agency to perform the match. The disclosure of records to the matching agency and any later disclosure of "hits" (by either the matching or the source agencies) must be done in accordance with the provisions of paragraph (b) of the Privacy Act.

5. Hit. The identification, through a matching program, of a specific individual.

E. GUIDELINES FOR AGENCIES PARTICIPATING IN MATCHING PROGRAMS. Agencies should acquire and disclose matching records and conduct matching programs in accordance with the provisions of this section and the Privacy Act.

1. Disclosing Personal Records for Matching Programs.

a. To another federal agency. Source agencies are responsible for determining whether or not to disclose personal records from their systems and for making sure they meet the necessary Privacy Act disclosure provisions when they do. Among the factors source agencies should consider are:

(1) Legal authority for the match;

(2) Purpose and description of the match;

(3) Description of the records to be matched;

(4) Whether the record subjects have consented to the match; or whether disclosure of records for the match would be compatible with the purpose for which the records were originally collected; that is, whether disclosure under a "routine use" would be appropriate; whether the soliciting agency is seeking the records for a legitimate law enforcement activity--whichever is appropriate; or any other provision of the Privacy Act under which disclosure may be made;

(5) Description of additional information which may be subsequently disclosed in relation to "hits";

(6) Subsequent actions expected of the source (for example, verification of the identity of the "hits" or follow-up with individuals who are "hits").

(7) Safeguards to be afforded the records involved, including disposition.

b. If the agency is satisfied that disclosure of the records would not violate its responsibilities under the Privacy Act, it may proceed to make the disclosure to the matching agency. It should ensure that only the minimum information necessary to conduct the match is provided. If disclosure is to be made pursuant to a "routine use" (Section (b)(3) of the Privacy Act), it should ensure that the system of records contains such a use, or it should publish a routine use notice in the Federal Register. The agency should also be sure to maintain an accounting of the disclosures pursuant to Section (c) of the Privacy Act.

c. To a nonfederal entity. Before disclosing records to a nonfederal entity for a matching program to be carried out by that entity, a source agency should, in addition to all of the consideration in paragraph E.1.a., above also make reasonable efforts, pursuant to Section (e)(6) of the Privacy Act, to "assure that such records are accurate, complete, timely, and relevant for agency purposes."

2. Written Agreements. Before disclosing to either a federal or nonfederal entity, the source agency should require the matching entity to agree in writing to certain conditions governing the use of the matching file; for example, that the matching file will remain the property of the source agency and be returned at the end of the matching program (or destroyed as appropriate); that the file will be used and accessed only to match the file or files previously agreed to; that it will not be used to extract information concerning "non-hit" individuals for any purpose, and that it will not be duplicated or disseminated within or outside the matching agency unless authorized in writing by the source agency.

3. Performing Matching Programs.

(a) Matching agencies should maintain reasonable administrative, technical, and physical security safeguards on all files involved in the matching program.

(b) Matching agencies should insure that they have appropriate systems of records including those containing "hits," and that such systems and any routine uses have been appropriately noticed in the Federal Register and reported to OMB and the Congress, as appropriate.

4. Disposition of Records.

a. Matching agencies will return or destroy source matching files (by mutual agreement) immediately after the match.

b. Records relating to hits will be kept only so long as an investigation, either criminal or administrative, is active, and will be disposed of in accordance with the requirements of the Privacy Act and the Federal Records Schedule.

5. Publication Requirements.

a. Agencies, before disclosing records outside the agency, will publish appropriate "routine use" notices in the Federal Register, if necessary.

b. If the matching program will result in the creation of a new or the substantial alteration of an existing system of records, the agency involved should publish the appropriate Federal Register notice and submit the requisite report to OMB and the Congress pursuant to OMB Circular No. A-108.

6. Reporting Requirements.

a. As close to the initiation of the matching program as possible, matching agencies shall publish in the Federal Register a brief public notice describing the matching program. The notice should include:

(1) The legal authority under which the match is being conducted;

(2) A description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose or purposes for which the program is being conducted, and the procedures to be used in matching and following up on the "hits";

(3) A complete description of the personal records to be matched, including the source or sources, system of records identifying data, date or dates and page number of the most recent Federal Register full text publication when appropriate;

(4) The projected start and ending dates of the program;

(5) The security safeguards to be used to protect against unauthorized access or disclosure of the personal records; and

(6) Plans for disposition of the source records and "hits."

7. Agencies should send a copy of this notice to the Congress and to OMB at the same time it is sent to the Federal Register.

a. Agencies should report new or altered systems of records as described in paragraph E.5.b., above, as necessary.

b. Agencies should also be prepared to report on matching programs pursuant to the reporting requirements of either the Privacy Act or the Paperwork Reduction Act. Reports will be solicited by the Office of Information and Regulatory Affairs and will focus on both the protection of individual privacy and the government's effective use of information technology. Reporting instructions will be disseminated to the agencies as part of either the reports required by paragraph (p) of the Privacy Act, or Section 3514 of Pub. L. 96-511.

8. Use of Contractors. Matching programs should, as far as practicable, be conducted "in-house" by federal agencies using agency personnel, rather than by contract. When contractors are used, however,

a. The matching agency should, consistent with paragraph (m) of the Privacy Act, cause the requirements of that Act to be applied to the contractor's performance of the matching program. The contract should include the Privacy Act clause required by Federal Personnel Regulation Amendment 155 (41 CFR 1-1.337-5);

b. The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards, and guidelines issued by OMB, GSA, and the Department of Commerce;

c. The terms of the contract should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor's own use;

d. Contractor personnel involved in the matching program shall be made explicitly aware of their obligations under the Act and of these guidelines, agency rules, and any special safeguards in relation to each specific match performed.

e. Any disclosures of records by the agency to the contractor should be made pursuant to a "routine use" (5 U.S.C. 552a (b)(3)).

F. IMPLEMENTATION AND OVERSIGHT. OMB will oversee the implementation of these guidelines and shall interpret and advise upon agency proposals and actions within their scope, consistent with Section 6 of the Privacy Act.